GFI Product Manual

GFI EventsManager™

Event log monitoring, management and archiving

ReportPack User Manual

http://www.gfi.com
info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI EventsManager ReportPack is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Document Version: ESMRP-UM-EN-1.03.00

Last updated: 28 June 2011

Contents

1 Introduction 1

1.1 About GFI ReportCenter 1
1.2 About the GFI EventsManager ReportPack 2
1.3 Components of the GFI EventsManager ReportPack 3
1.4 Key features 4

2 Installation 7

2.1 System requirements 7
2.2 Installation procedure 7
2.3 Launching the GFI EventsManager reports for GFI ReportCenter 9
2.4 Selecting a product 9

3 Getting started: Default reports 11

3.1 Introduction 11
3.2 Generating a default report 12
3.3 Analyzing the generated report 14
3.4 Adding default reports to the list of favorite reports 15

4 Custom reports 17

4.1 Introduction 17
4.2 Creating a new custom report 17
4.3 Configuring data filter conditions 19
4.4 Run a custom report 23
4.5 Editing a custom report 24
4.6 Deleting a custom report 24
4.7 Adding custom reports to the list of favorite reports 25

5 Scheduling reports 27

5.1 Introduction 27
5.2 Scheduling a report 27
5.3 Configuring advanced settings 29
5.4 Viewing the list of scheduled reports 32
5.5 Viewing the scheduled reports activity 33
5.6 Enable/disable a scheduled report 34
5.7 Editing a scheduled report 34
5.8 Deleting a scheduled report 34
5.9 Example: Scheduling a report 35

6 Configuring default options 39

6.1 Introduction 39
6.2 Configuring database source 39
6.3 Viewing the current database source settings 41
6.4 Configuring default scheduling settings 41

7 Exporting and Importing Configuration 43

7.1 Introduction 43
7.2 Exporting settings 43
7.3 Importing settings 44

8 General options 47
8.1 Entering your license key after installation 47
8.2 Viewing the current licensing details 48
8.3 Viewing the product ReportPack version details 48
8.4 Checking the web for newer builds 48

9 Appendix: Default Reports 49
9.1 Introduction 49
9.2 Account Usage Reports 49
9.3 Account Management 50
9.4 Policy Changes 51
9.5 Object Access 52
9.6 Application Management 52
9.7 Print Server 52
9.8 Windows Event Log system 53
9.9 Events Trend 53
9.10 All critical messages 54
9.11 Miscellaneous, Customizable reports 54
9.12 PCI DSS Compliance Reports 54
9.13 General and Security Requirements 59
9.14 SOX Compliance reports 61
9.15 HIPAA Compliance reports 62
9.16 GLBA compliance reports 63
9.17 Microsoft SharePoint reports 63

10 Troubleshooting 65
10.1 Introduction 65
10.2 Knowledge Base 65
10.3 Web Forum 65
10.4 Request technical support 65
10.5 Build notifications 65

Index 67

1 Introduction

1.1 About GFI ReportCenter

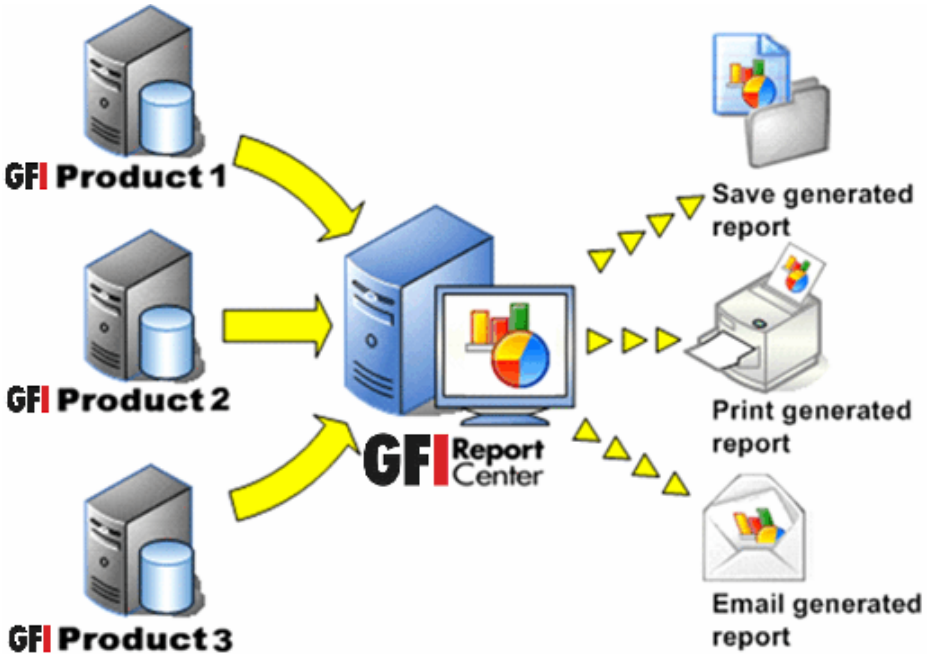


Figure 1 - Centralized reporting framework

GFI ReportCenter is a centralized reporting framework that enables you to generate various reports using data collected by different GFI products. The ReportPack can be downloaded and installed as an add-on to a GFI product.

Figure 2 - Several ReportPacks plugged into the GFI ReportCenter framework

A ReportPack plugs into the GFI ReportCenter framework; allowing you to generate, analyze, export and print the information generated through these reports.

1.2 About the GFI EventsManager ReportPack

The GFI EventsManager ReportPack is a full-fledged reporting companion to GFI EventsManager. It allows you to generate graphical IT-level, technical and management reports based on the hardware and software events recorded by GFI EventsManager. Hardware and software event sources include any networked component that can generate Syslog messages or record/log events to Windows and/or W3C event logs. These include computers, network devices, PABXs, and third party software solutions.

From management reports (Trend Reports) to technical staff reports (daily drill-down reports), the GFI EventsManager ReportPack provides you with the easy-to-view information required, to fully understand the events activity on your corporate network.

The GFI EventsManager ReportPack provides the following graphical and text based reports:

- Account Usage
- Account Management
- Policy Changes
- Object Access
- Application Management
- Print Server

- Windows Event Log system
- Events Trend
- All critical messages
- Miscellaneous, customizable reports.
- PCI DSS Compliance Reports
    - General and Security Requirements
    - SOX Compliance
    - HIPAA Compliance
    - GLBA Compliance
    - Microsoft SharePoint

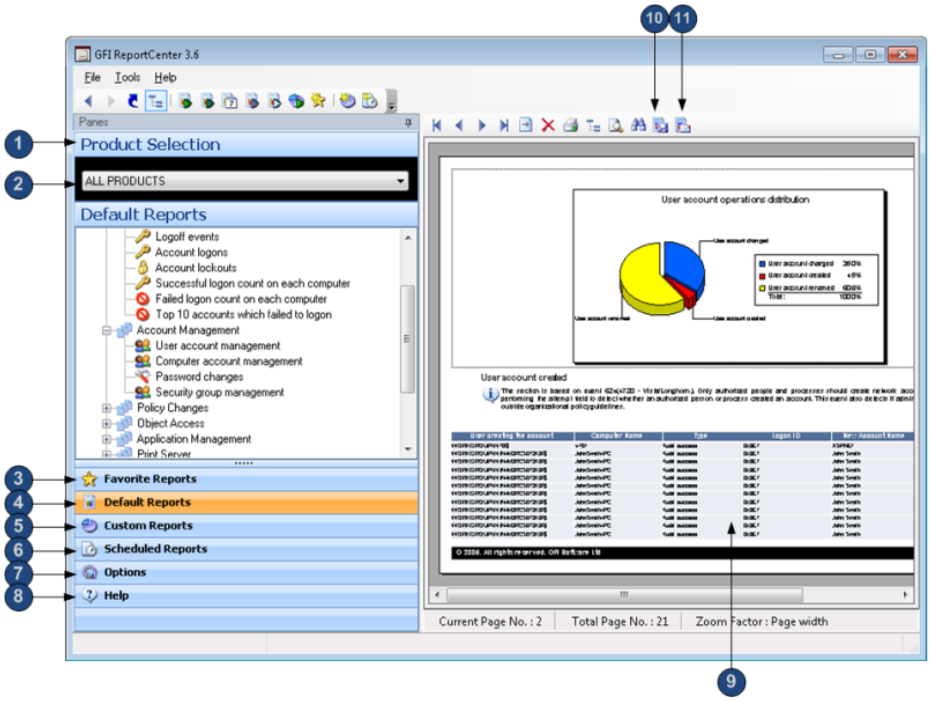
1.3 Components of the GFI EventsManager ReportPack

The GFI EventsManager ReportPack consists of:

- GFI ReportCenter framework
- GFI EventsManager default reports
- Report scheduling service.

1.3.1 GFI ReportCenter framework

The GFI ReportCenter framework is the management console that enables you to generate the specialized product reports contained in the ReportPack. The GFI ReportCenter framework offers a common application interface through which you can navigate, generate, customize and schedule reports.



Screenshot 1 - The GFI ReportCenter management console

The following table describes the components within the management console:

1	**Navigation Pane** – Use this pane to access the navigation buttons/configuration options provided with GFI ReportCenter.
2	**Product Selection drop-down list** – To generate reports for a specific product, select the product from the drop down list.
3	**Favorite Reports** – Use this navigation button to access your favorite/most used reports. For more information on how to add reports to this list, refer to the 'Adding default reports to the list of favorite reports' and 'Adding custom reports to the list of favorite reports' sections in this manual.
4	**Default Reports** – Use this navigation button to access the default list of reports, that can be generated for the selected product. For more information on default reports refer to the 'GFI EventsManager default reports' section in this manual.
5	**Custom Reports** – Use this navigation button to access the list of customized reports, that can be generated for the selected product. For more information on how to create custom reports refer to the 'Custom reports' chapter in this manual.
6	**Scheduled Reports** – Use this navigation button to access the list of scheduled reports for automatic generation and distribution. For more information on how to create scheduled reports refer to the 'Scheduling reports' chapter in this manual.
7	**Options** – Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.
8	**Help** – Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.
9	**Report Pane** - Use this multi-functional pane to: » View and analyze generated reports » Maintain the scheduled reports list » Explore samples and descriptions of default reports.
10	**Export** – Use this button to export generated reports to various formats including HTML, Adobe Acrobat (PDF), Excel (XLS), Word (DOC), and Rich Text Format (RTF).
11	**Send email** – Use this button to instantly distribute the last generated report via email.

GFI EventsManager default reports

The GFI EventsManager default reports are a collection of specialized pre-configured reports, that plug into the GFI ReportCenter framework. These reports present the events recorded by GFI EventsManager and allow for the generation of both graphical and tabular IT-Level, technical and management reports. Default reports can also serve as the base template for the creation of customized reports, that fit specific network-reporting requirements.

Report scheduling service

The report scheduling service controls the scheduling and automatic distribution of reports by email. Reports generated by this service can also be saved to a specific hard disk location in a variety of formats, that include DOC, PDF, RTF and HTML.

1.4 Key features

Centralized reporting

GFI ReportCenter is a one-stop, centralized reporting framework that enables the generation and customization of graphical and tabular reports for a wide array of GFI Products.

Wizard assisted configuration

Wizards are provided to assist you in the configuration, scheduling and customization of reports.

Report scheduling

With GFI ReportCenter, you can schedule reports to be generated on a pre-defined schedule as well as at specified intervals. For example, you can schedule lengthy reports to be generated after office hours. This allows you to maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Distribution of reports via email

GFI ReportCenter allows you to automatically distribute generated reports via email. In scheduled reports, this can be achieved automatically after the successful generation of a scheduled report.

Report export to various formats

By default, GFI ReportCenter allows you to export reports to various formats. Supported formats include HTML, PDF, XLS, DOC and RTF. When scheduling reports, you can optionally configure the preferred report output format. Different scheduled reports can also be configured to output generated reports to different file formats.

Default reports

The GFI EventsManager ReportPack ships with a default set of graphical and tabular reports. These reports can be generated without any further configuration effort immediately after the installation. The default reports in this ReportPack are organized into different report-type categories:

- Account Usage
- Account Management
- Policy Changes
- Object Access
- Application Management
- Print Server
- Windows Event Log system
- Events Trend
- All critical messages
- Miscellaneous, customizable reports.
- PCI DSS Compliance Reports
- General and Security Requirements
- SOX Compliance
- HIPAA Compliance
- GLBA Compliance
- Microsoft SharePoint

Report customization

The default reports that ship with every ReportPack can serve as the base template for the creation of customized reports. Report customization is achieved by building up custom data filters that will analyze the data source and filter the information that matches specific criteria. In this way, you create reports tailored to your reporting requirements.

Favorites

GFI ReportCenter allows you to create bookmarks to your most frequently used reports – both default and custom.

Printing

By default, all reports generated by GFI ReportCenter are printer friendly and can be printed through the windows printing services provided by the system were GFI ReportCenter is installed.

2 Installation

2.1 System requirements

Install the GFI EventsManager ReportPack on a computer that meets the following requirements:

- Microsoft Windows 2008, 2003 (SP2), 2000 (SP4), XP (SP2), Microsoft Windows Vista, Microsoft Windows 7.
- .NET framework 2.0
- Internet Explorer 5.1 or higher
- GFI EventsManager 8.x or higher

The GFI EventsManager ReportPack only allows you to generate reports for data contained in the SQL Server database backend of GFI EventsManager.

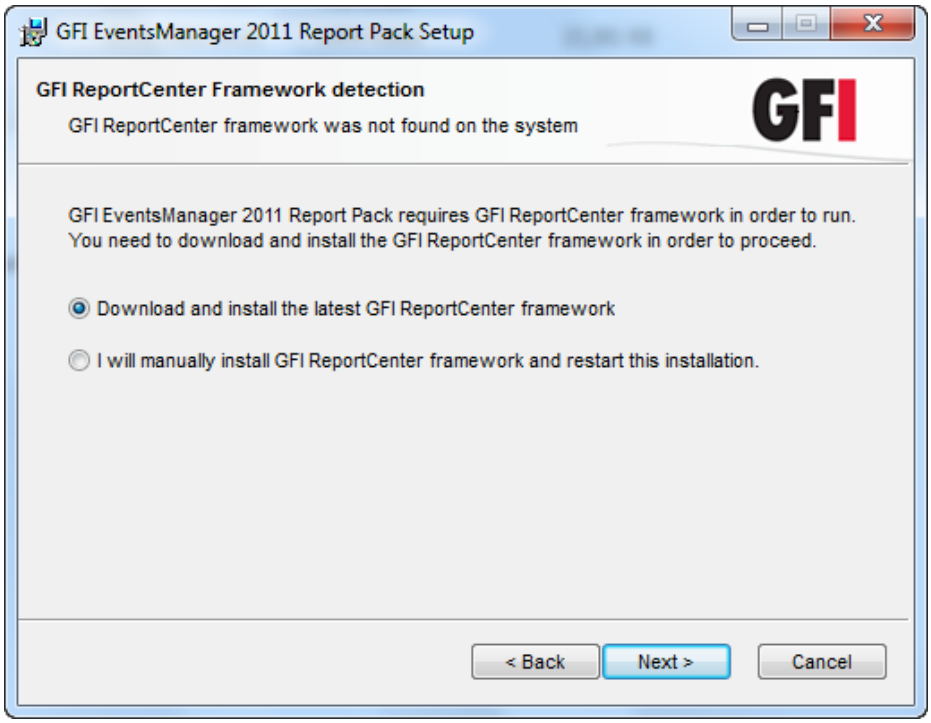
2.2 Installation procedure

The GFI EventsManager ReportPack includes an installation wizard that will assist you through the installation process. During the installation process, this wizard will:

- Verify that you are running the latest version of the GFI ReportCenter framework; if you are installing the framework for the first time or the currently installed framework version is outdated, the installation wizard will automatically download the latest one for you.
- Automatically install all the required components distributed including the GFI ReportCenter framework, the GFI EventsManager default reports and the Report Scheduling service.

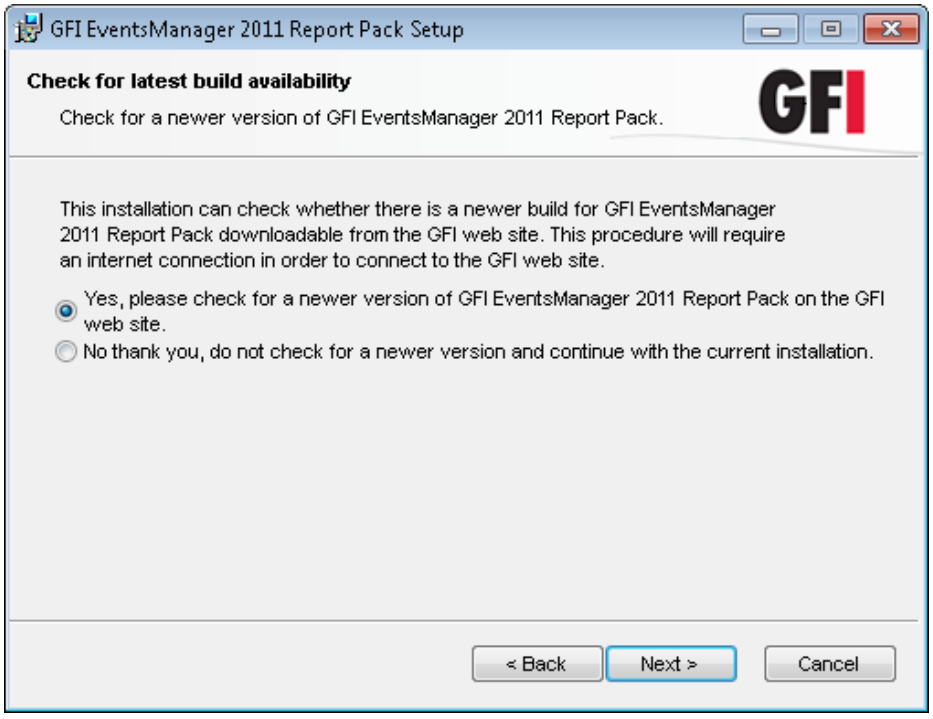
To start the installation:

1. Double-click on the report pack executable file and in the welcome screen, click **Next** to start the installation.


GFI EventsManager 2011 Report Pack Setup
GFI ReportCenter Framework detection
GFI ReportCenter framework was not found on the system
GFI
GFI EventsManager 2011 Report Pack requires GFI ReportCenter framework in order to run.
You need to download and install the GFI ReportCenter framework in order to proceed.
Download and install the latest GFI ReportCenter framework
I will manually install GFI ReportCenter framework and restart this installation.
< Back
Next >
Cancel

Screenshot 2 - GFI ReportCenter framework detection dialog

2. If the current version of GFI ReportCenter framework is not compatible with the GFI EventsManager ReportPack, you will be prompted to download and install an updated version. Select **Download and install the GFI ReportCenter…** and click **Next.**

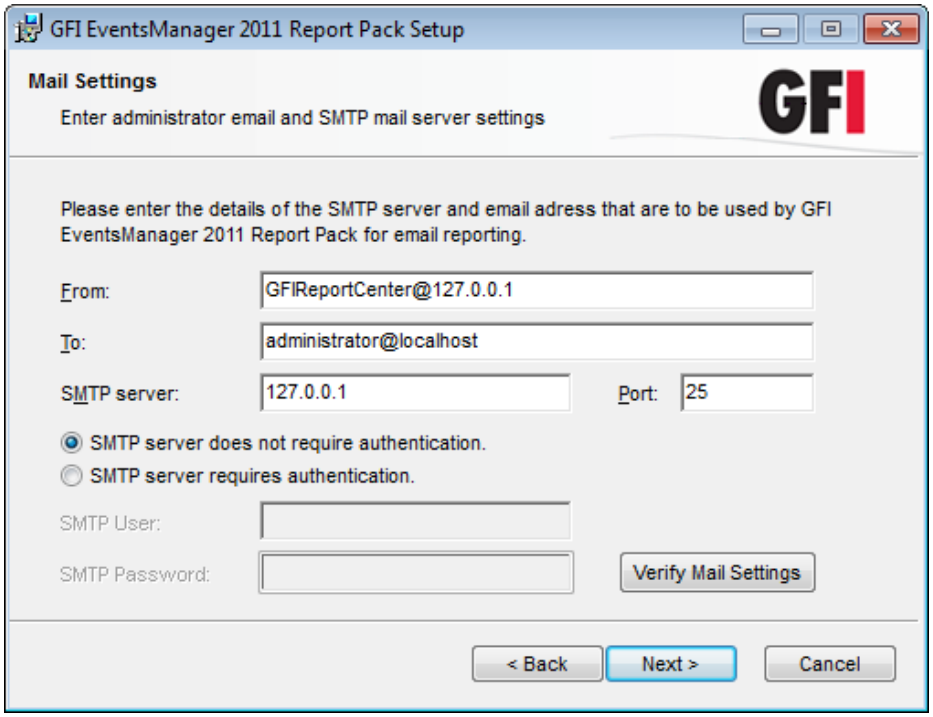

GFI EventsManager 2011 Report Pack Setup
Check for latest build availability
Check for a newer version of GFI EventsManager 2011 Report Pack.
GFI
This installation can check whether there is a newer build for GFI EventsManager 2011 Report Pack downloadable from the GFI web site. This procedure will require an internet connection in order to connect to the GFI web site.
Yes, please check for a newer version of GFI EventsManager 2011 Report Pack on the GFI web site.
No thank you, do not check for a newer version and continue with the current installation.
< Back
Next >
Cancel

Screenshot 3 - Check for latest build availability

3. Choose whether you want the installation wizard to search for a newer build of the GFI EventsManager ReportPack on the GFI website and click **Next.**

4. In the license dialog, read the licensing agreement carefully. Select the **I accept the Licensing agreement** option and click **Next.**

5. Specify the details of the SQL Server that is hosting your GFI EventsManager database backend, and click **Next.**



Screenshot 4 - Email configuration dialog

6. Specify the default email settings that will be used for report distribution and click **Next**.

7. Specify the product installation path or click **Next** to install GFI Report Pack in the default path. The installation will need approximately 100 MB of free disk space.

8. The installation wizard is now ready to copy the required files and finalize the installation. Click **Next**.

2.3 Launching the GFI EventsManager reports for GFI ReportCenter

Following the installation, launch the GFI EventsManager Reports for GFI ReportCenter from **Start ► Programs ► GFI ReportCenter ► EventsManager 2010 ReportPack**.

2.4 Selecting a product

When more than one product ReportPack is installed, use the **Product Selection** drop down list to select the GFI product ReportPack to be used.

Screenshot 5 - Product Selection drop down list

For example, to run the reports provided in the GFI EventsManager ReportPack:

1. Launch GFI ReportCenter from **Start ► Program Files ► GFI ReportCenter**.

2. Select **GFI EventsManager 2010 ReportPack** from the **Product Selection** drop down list.

Select the **ALL PRODUCTS** option to display and navigate all the ReportPacks that are currently installed in GFI ReportCenter.

3 Getting started: Default reports

3.1 Introduction

After installing the GFI EventsManager ReportPack, a number of specialized pre-configured reports can immediately be generated on the data stored in the database backend of GFI EventsManager. These default reports are organized into the following categories:

- **Account Usage Reports** - Use the reports in this category to identify user logon issues. The event details shown in these reports include successful/failed user logons and locked user accounts.
- **Account Management Reports** - Use the reports in this category to generate a graphical overview of important events that took place across your entire network. The event details shown in these reports include changes in user and computer accounts as well as changes in security group policies.
- **Policy Changes Reports** - Use the reports in this category to identify policy changes effected on your network.
- **Object Access Reports** - Use the reports in this category to identify object access issues. The event details shown in these reports include successful/failed object access and objects that have been deleted.
- **Application Management Reports** - Use the reports in this category to identify faulty applications and application installation and removal issues. The event details shown in these reports include applications that have been installed or removed as well as applications, which are crashing and hanging.
- **Print Server Reports** - Use the reports in this category to display details related to printing events. Details provided in these reports include documents that have been printed, the users that triggered the printing event and the date/time when the printing operation took place.
- **Windows Event Log System Reports** - Use the reports in this category to identify audit failures and important Windows event log issues. Details provided in these reports include the starting and stopping of event log services, clear log operations as well as errors generated during event logging.
- **Events Trend Reports** - Use the reports in this category to display statistical information related to event generation. Charts provided enumerate the 10 computers and users with most events. Other reports provide event counts on a network-wide basis as well as on a computer-by-computer basis. Reports in this category can be generated for each main time – by hour, day, week or month.
- **All critical reports** - Use the reports in this category to display information related to critical Windows events, Syslog, W3C, Custom Events, SNMP Traps and SQL Server Audit events. The charts provided enumerate the 10 most critical events.
- **Miscellaneous**, **Customizable reports** - Use the reports in this category to generate reports that offer broad customization. These can be used to generate reports based on any Windows event log, using filtering conditions and grouping modes that are not covered by the other default reports.
- **PCI DSS Compliance Reports** - Use the reports in this category to generate various reports by the PCI DSS compliance standards.
- **General and Security Requirements** - Use the reports in this category to generate various reports required by several GCSx Code of Connection memos

» **LOGbinder SP reports** – Use the reports in this category to generate reports related to Microsoft SharePoint audit events.

GFI EventsManager default reports are accessed by clicking on the **Default Reports** navigation button provided in the management.

3.2 Generating a default report

To generate a default report:

1. Click on the **Default Reports** navigation button to launch the list of default reports available.

Screenshot 6 - Selecting the data set period

2. Right-click on the report to be generated, select **Run** and specify the event date/time period that will be covered by the report.

Example 1: Generating a "Failed logons" report based today's data.

This example demonstrates how to generate a failed logons report based on the events that were recorded today:

1. Click on the **Default Reports** navigation button to launch the list of available reports.

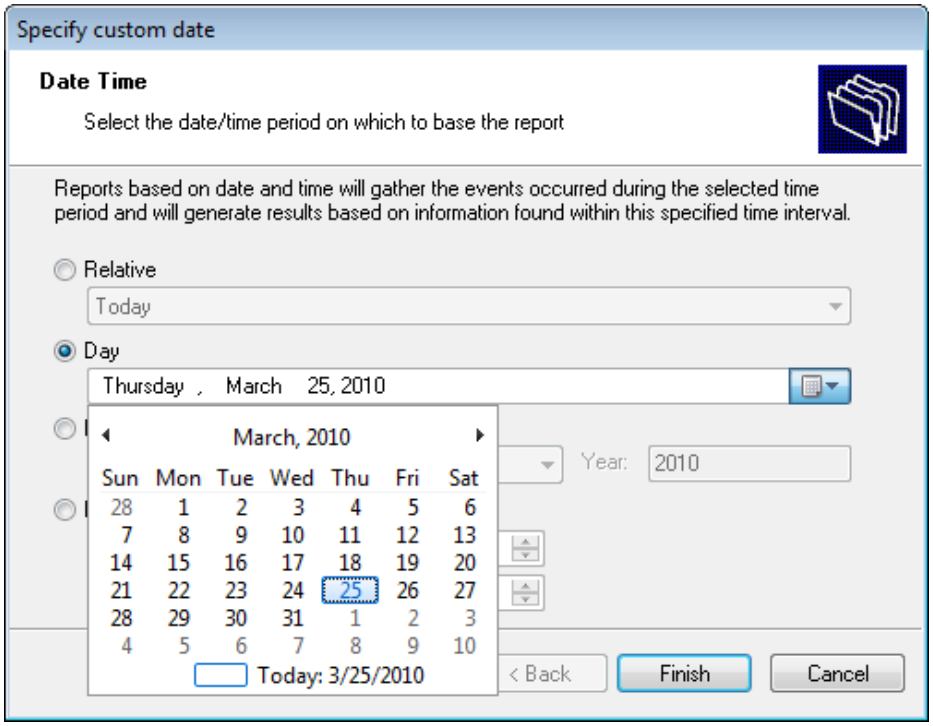
2. Right-click on **Failed logons** and select **Run ► For Today**.

Example 2: Generating a "Failed logons" report based on that data collected on a particular day.

This example demonstrates how to generate a failed logons report based on the events that were recorded on the March 25, 2010.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on **Failed logons** and select **Run ► For Custom Date**.


Specify custom date
Date Time
Select the date/time period on which to base the report
Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.
Relative
Today
Day
Thursday , March 25, 2010
March, 2010
Sun Mon Tue Wed Thu Fri Sat
28 1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31 1 2 3
4 5 6 7 8 9 10
Today: 3/25/2010
Year: 2010
< Back
Finish
Cancel

Screenshot 7 - Configuring custom date/time period

3. Select the **Day** option and expand the provided drop down to display the calendar.

4. Navigate to the required month (i.e. March) and select the required day (i.e. 1).

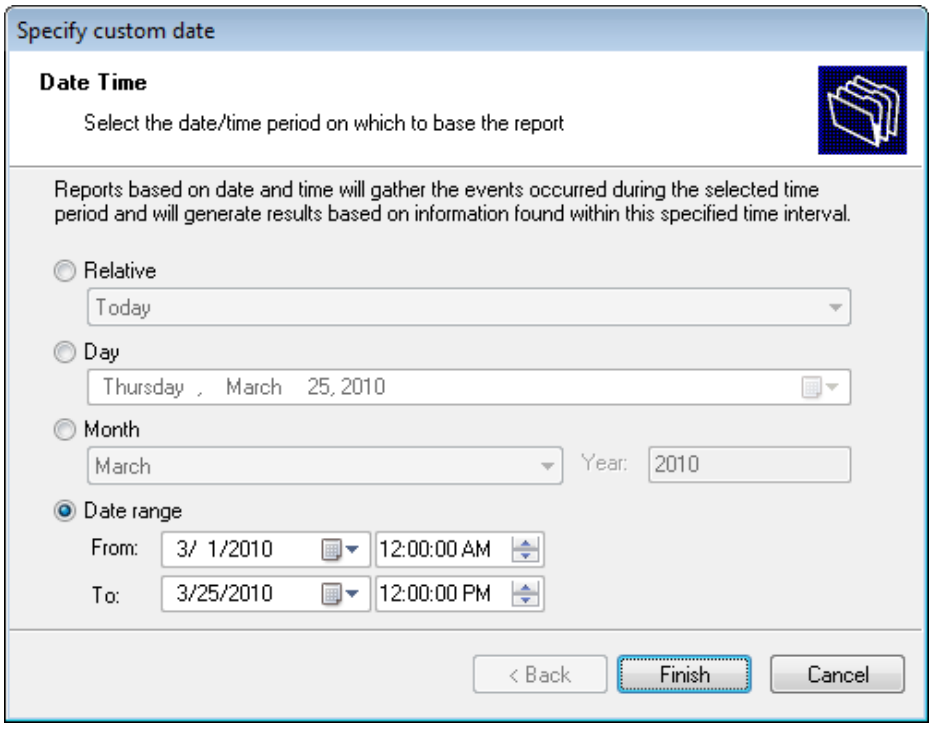
5. Click **Finish** to generate the report.

Example 3: Generating a "Failed logons" report based on data collected over a specific date/time period.

This example demonstrates how to generate a failed logons report based on the events recorded between March 1, 2010 and March 25, 2010.

1. Click on the **Default Reports** navigation to launch the list of available reports.

2. Right-click on **Failed logons** and select **Run ► For Custom Date**.


Specify custom date
Date Time
Select the date/time period on which to base the report
Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.
Relative
Today
Day
Thursday , March 25, 2010
Month
March
Year: 2010
Date range
From: 3/ 1/2010 12:00:00 AM
To: 3/25/2010 12:00:00 PM
< Back
Finish
Cancel

Screenshot 8 - Configuring custom date/time period

3. Select the **Date range** option and specify the required parameters:

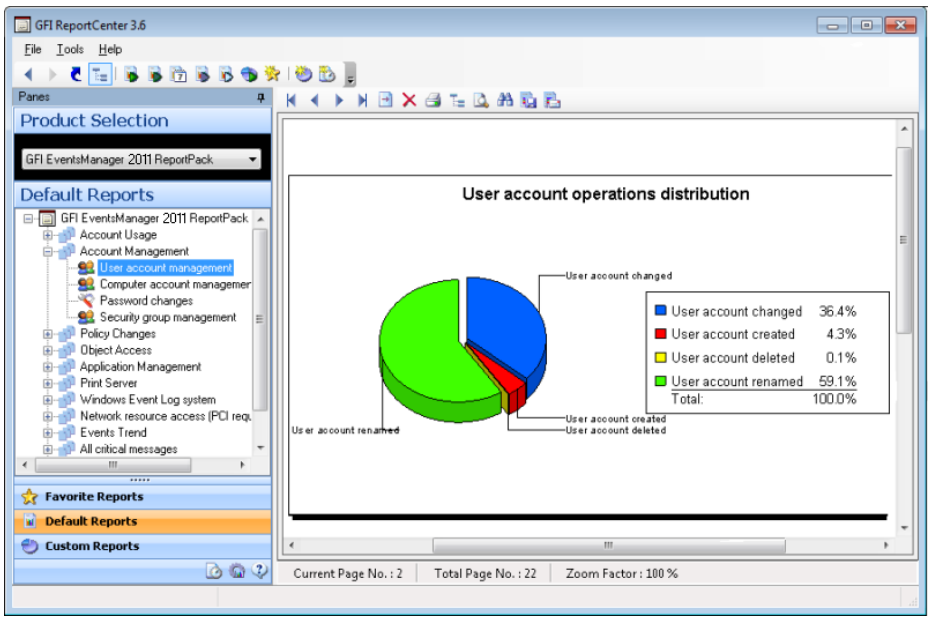
» **From** –3/1/2010 12:00:00 AM.

» **To** – 3/25/2010 12:00:00 PM.

Date and time format are based on the regional settings configured on your computer.

4. Click **Finish** to generate the report.

3.3 Analyzing the generated report



Screenshot 9 - Generated reports are displayed in the right pane of the management console

Generated reports are shown in the right pane of the GFI ReportCenter. Use the toolbar at the top of the report pane to access common report related functions:

Report browsing options

Browse the generated report page by page.

Zoom in/Zoom out.

Search the report for particular text or characters.

Go directly to a specific page.

Breakdown the report into a group tree (e.g. by date/time).

Print report.

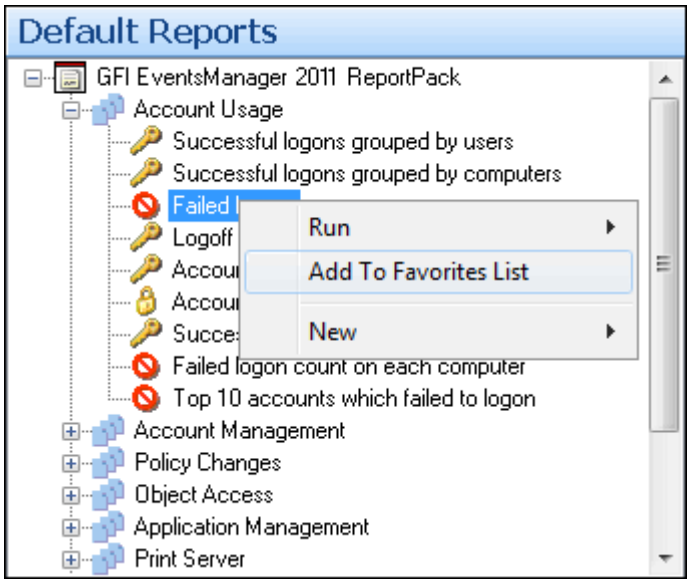
Report storage and distribution options

Export the generated report to a specific file format.

Distribute the generated report via email.

For information on how to configure report storage and distribution options, refer to the Configuring advanced settings section in this manual.

3.4 Adding default reports to the list of favorite reports



Screenshot 10 - Favorite Reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a default report to the list of favorite reports:

1. Click on the **Default Reports** navigation button to launch the list of available reports.

2. Right-click on the default report to be added to the favorites, and select **Add to favorites list**.

3. Click **Yes** to confirm.

4 Custom reports

4.1 Introduction

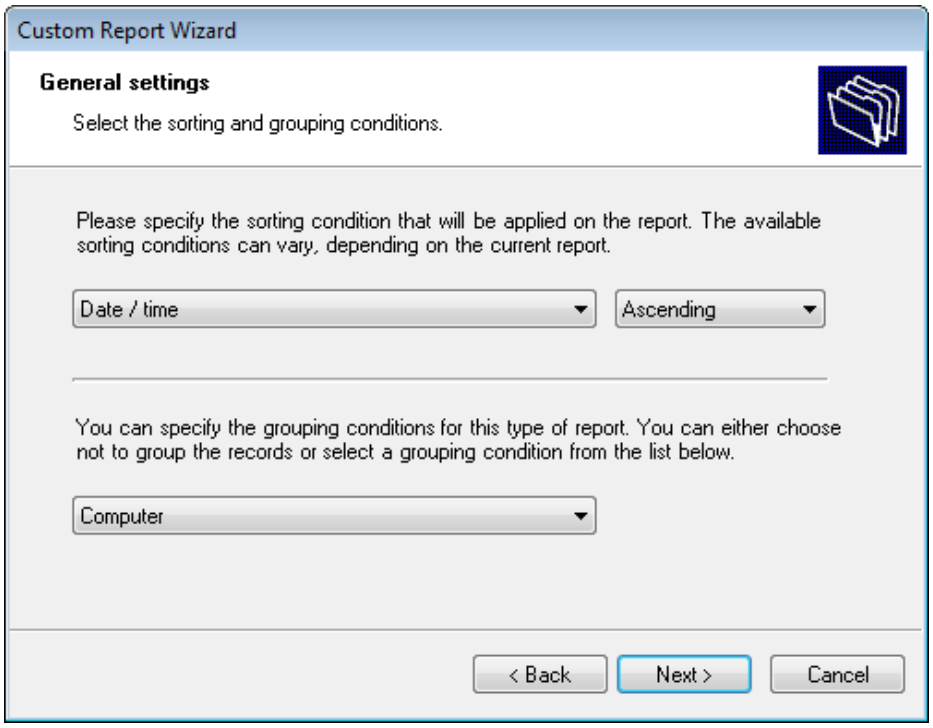
GFI ReportCenter allows you to create custom reports that are tailored to your reporting requirements. This is achieved by building up custom data filters that will analyze the data source and filter out the information that matches the specified criteria.

4.2 Creating a new custom report

To create a custom report:

1. Click on the **Default Reports** navigation button.

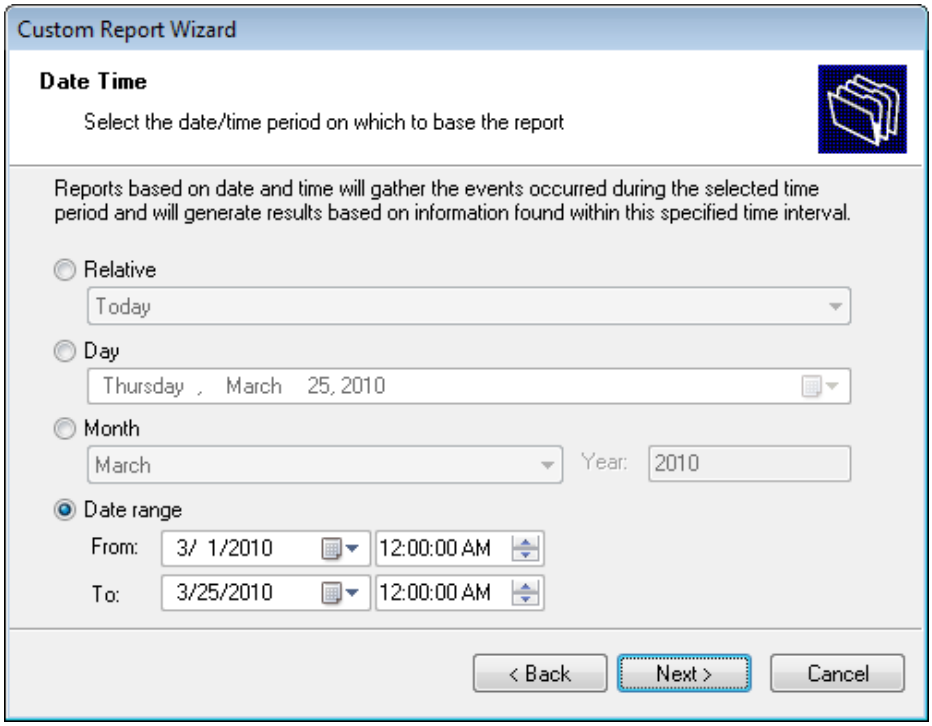
2. Right-click on the default report to be used as template and select **New ► Custom Report**.


Custom Report Wizard
General settings
Select the sorting and grouping conditions.
Please specify the sorting condition that will be applied on the report. The available sorting conditions can vary, depending on the current report.
Date / time
Ascending
You can specify the grouping conditions for this type of report. You can either choose not to group the records or select a grouping condition from the list below.
Computer
< Back
Next >
Cancel

Screenshot 11 - Sorting and grouping conditions to be applied to the report

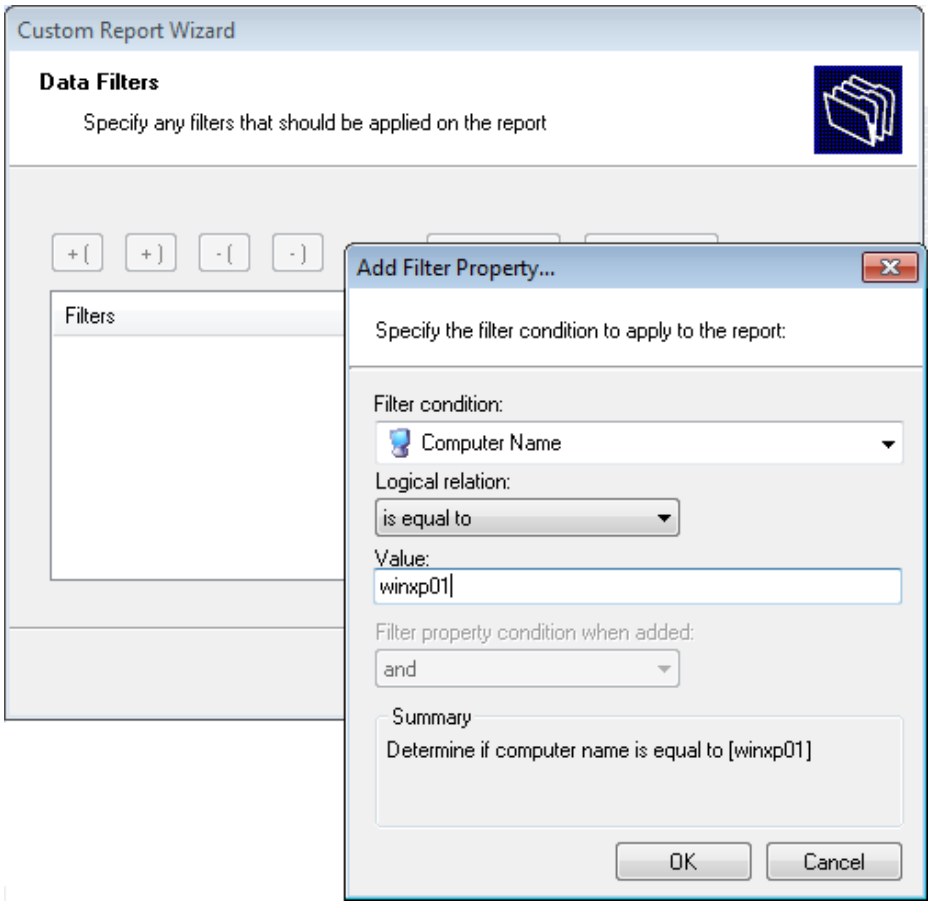
3. Specify how the information will be sorted in your report.

4. Specify how the information will be grouped in your report.


Custom Report Wizard
Date Time
Select the date/time period on which to base the report
Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.
Relative
Today
Day
Thursday , March 25, 2010
Month
March
Year: 2010
Date range
From: 3/ 1/2010 12:00:00 AM
To: 3/25/2010 12:00:00 AM
< Back
Next >
Cancel

Screenshot 12 - Selecting the data source to use

5. Select the data source that will be used to generate the custom report (based on the date/time period).



Screenshot 13 - Specifying data filter conditions

6. Configure the data filter conditions that will be applied against the selected data source. Click **Next**.

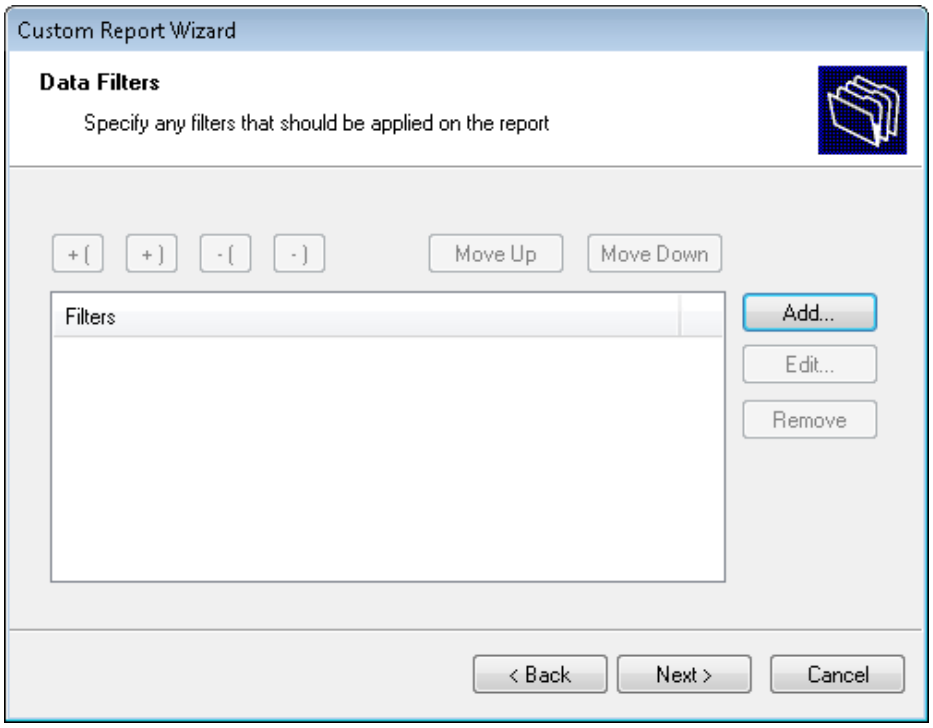
For more information on how to configure filter conditions, refer to the section Configuring data filter conditions in this manual.

7. Specify a name and description for the customized report. Click **Next**.

8. Click **Finish** to save the configuration settings.

4.3 Configuring data filter conditions

Use data filter conditions to specify the events that will be included in the report. Only the events that match the specified criteria will be processed and displayed in the report.

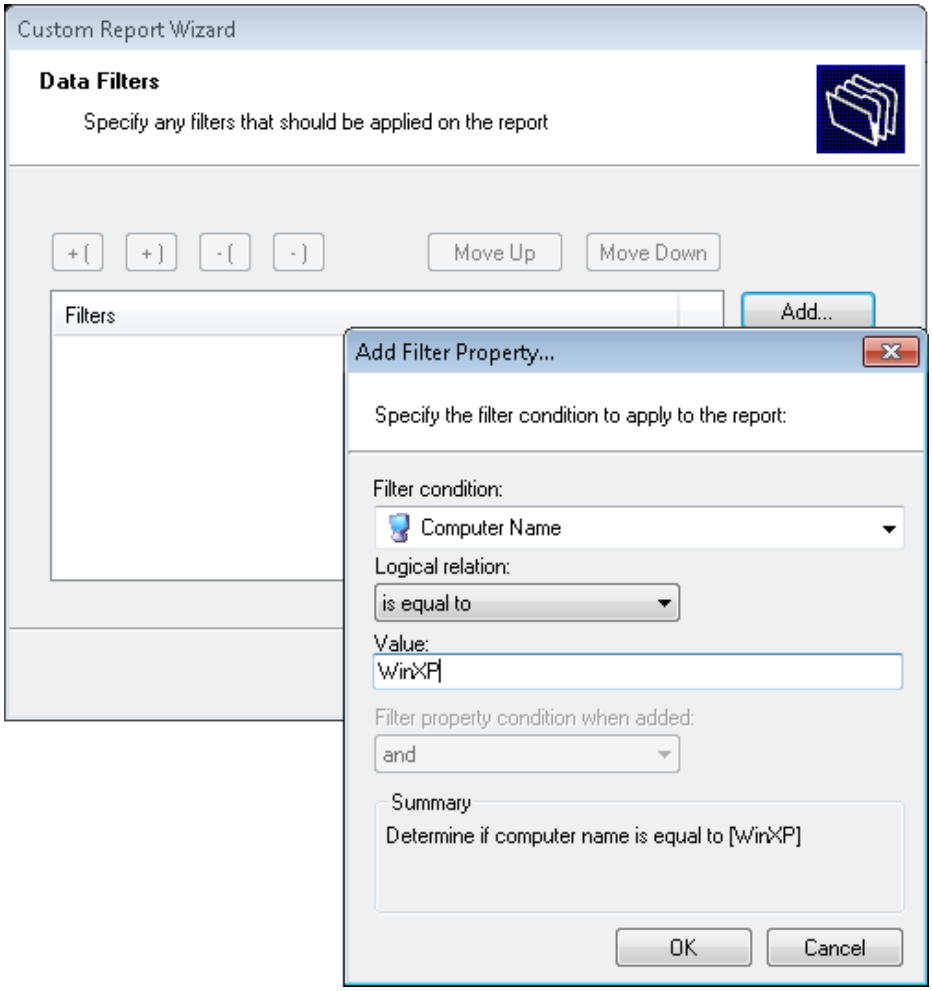


Screenshot 14 - Custom Report Wizard: Filters dialog

Click on the **Add…** to launch the **Add Filter Property** dialog and configure the following conditions:

- **Filter condition** – Specify the data source area were the filter will focus (for example, select **Computer Name** to filter the events data related to a particular computer).
- **Condition** – Specify the condition comparison parameter.
- **Value** – Specify the string that will be compared to the source data.

For example to generate a report that contains only information related to a workstation called “WinXP”, configure your filter parameters as shown below:



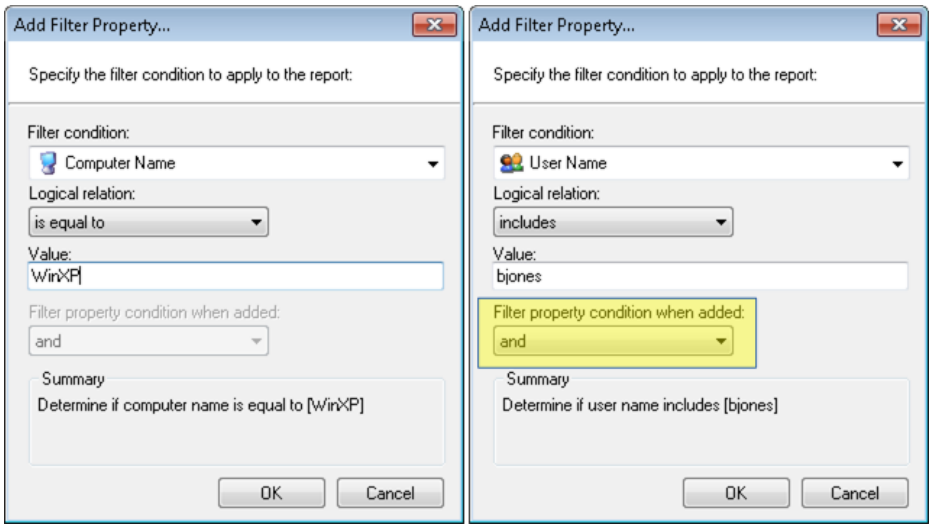
Screenshot 15 - Filter conditions configuration dialog

For more specific reports, you can limit the range of information to be displayed by tightening your conditions/search criteria. This is achieved by configuring and applying multiple data filters against the selected data source. When more than one filter is used, specify how these filters will be logically linked. This is achieved by selecting a logical grouping condition from **Filter property condition…** drop down list.

- Select **And** to include ALL the scan data information that satisfies ALL of the conditions specified in the filters.
- Select **Or** to include ALL the scan data information that matches at least one of the specified filter conditions.

Example: Using multiple filters

Consider the situation were a custom report has two filters configured as follows:



Screenshot 16 - Using multiple filters

Parameters	Filter 1	Filter 2
Filter condition	Computer Name	User Name
Logical relation	Is equal to	Includes
Value	WinXP	Bjones

The data, that will be included in this custom report, will vary according to how these filters will be applied against your data. This is defined through the **Filter property condition…** drop-down.

Filters applied			Data output
Filter 1	and	Filter 2	The report will show: » All the events by users called 'bjones' on the computer called 'WinXP'.
Filter 1	or	Filter 2	The report will show: » All the events generated by users called 'bjones' - (no matter on which computer the connections were made) AND » All events related to the computer called 'WinXP' - (no matter who the users are).

Example: Creating a custom report based on data collected during a particular month

This example demonstrates how to generate a failed logon report called 'Failed logons in March 2010'. This report will be based on the events:

» Collected from the computer called 'WinXp01'

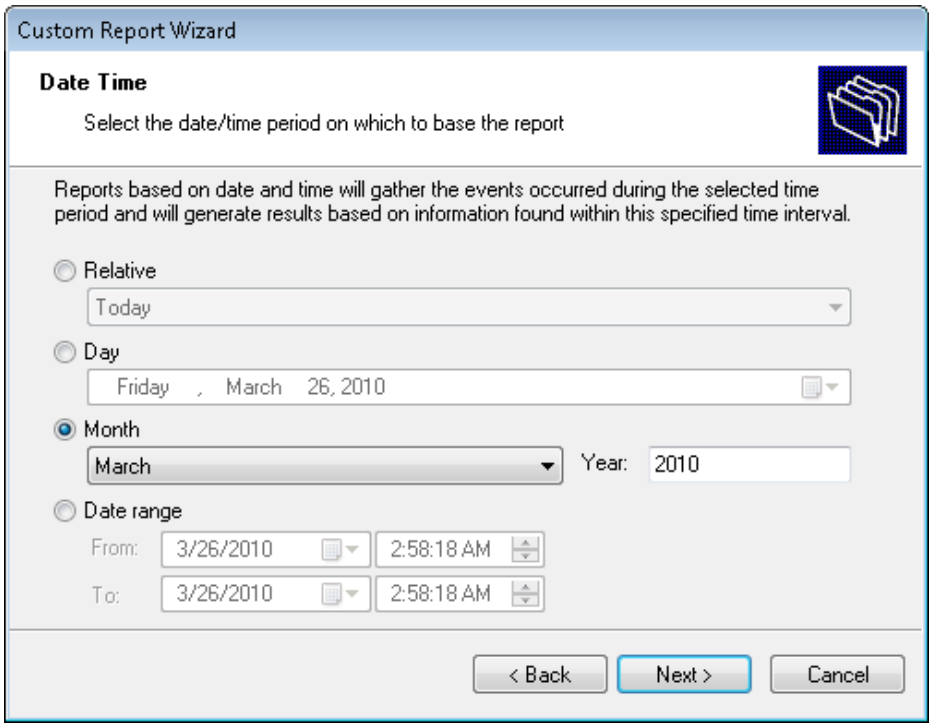
» Generated by the user account 'bjones'

» Recorded during the month of 'March 2010'.

To create this report:

1. Click on the **Default Reports** navigation button.

2. Right-click on the report to be customized and select **New ► Custom Report**. Click **Next**.



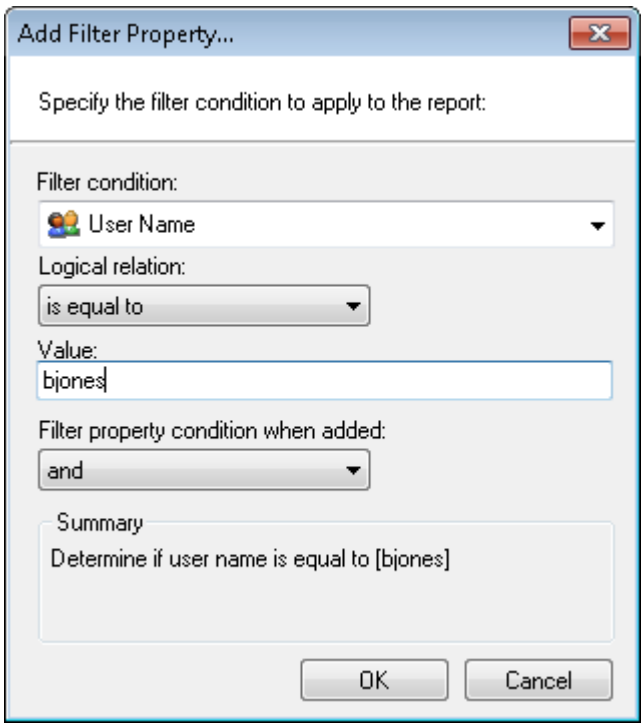
Screenshot 17 - Selecting the data source to use

3. Select the **Month** option and specify the following parameters:

» **Month**: March.

» **Year**: 2010.

4. Click **Next**..



Screenshot 18 - Filter conditions dialog(s) one

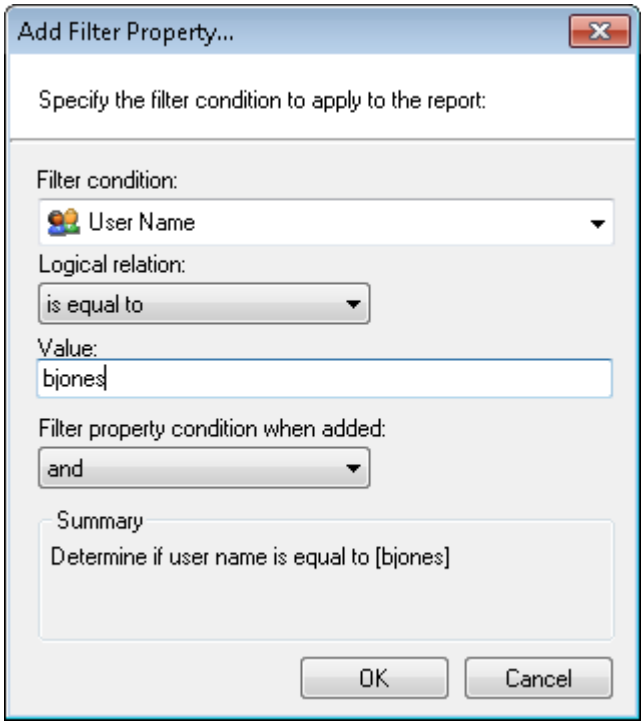
5. Click on the **Add...** button and configure the parameters of filter 1 as follows:

» **Filter condition**: Computer Name

» **Condition**: Equal to

» **Value**: WinXp01.

6. Click **OK** to finalize your filter configuration settings.



Screenshot 19 - Filter conditions dialog(s) two

7. Click again on the **Add…** button and configure the parameters of filter 2 as follows:

» **Filter condition**: Account

» **Condition**: is equal to

» **Value**: bjones

» **Filter** Property condition: and.

8. Click **OK** to finalize your filter configuration settings.

9. Click **Next** and specify the following parameters:

» **Report Name**: Failed logons in March 2010

» **Report Title:** Failed logons by bjones on computer WinXp01

» **Report Description**: This report shows the failed logons made by user Bob Jones on computer WinXp01 during March 2010.

10. Click **Next**.

11. Click **Finish** to finalize your custom report configuration settings.

4.4 Run a custom report

To run a custom report:

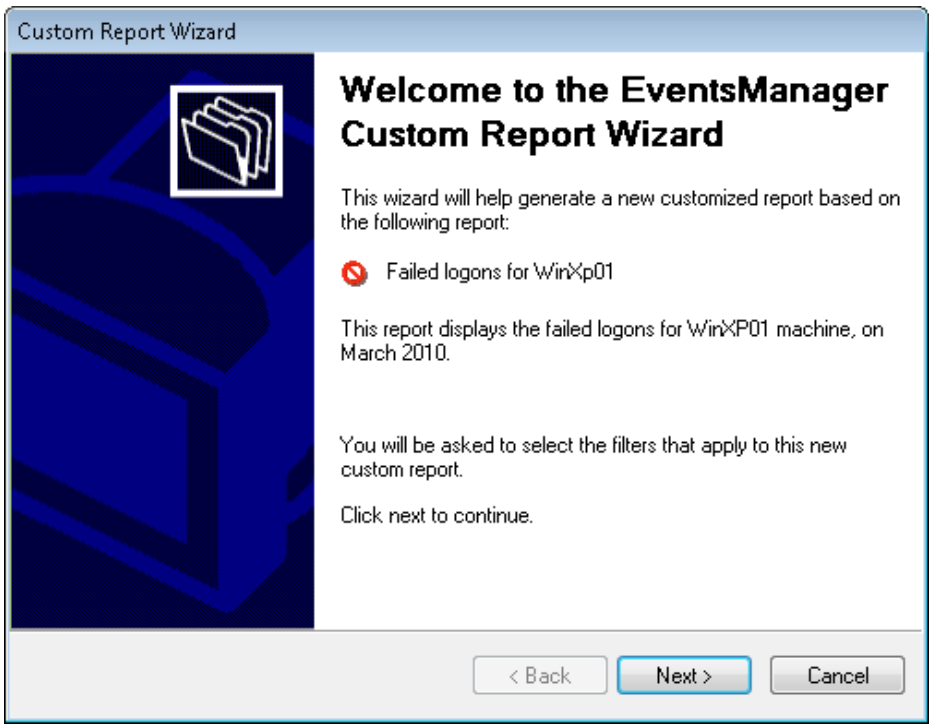
1. Click on the **Custom Reports** navigation button.

2. Right-click on the custom report that will be generated and select **Generate**.

4.5 Editing a custom report

To edit the configuration settings of a custom report:

1. Click on the **Custom Reports** navigation button.


Custom Report Wizard
Welcome to the EventsManager Custom Report Wizard
This wizard will help generate a new customized report based on the following report:
Failed logons for WinXp01
This report displays the failed logons for WinXP01 machine, on March 2010.
You will be asked to select the filters that apply to this new custom report.
Click next to continue.
< Back
Next >
Cancel

Screenshot 20 - Custom Report Wizard: Welcome dialog

2. Right-click on the custom report to be modified and select **Edit**. This will launch the 'Custom Reports Wizard' were you can make the required changes.

For more information on how to configure, the parameters of a custom report refer to the 'Creating a custom report' section in this chapter.

4.6 Deleting a custom report

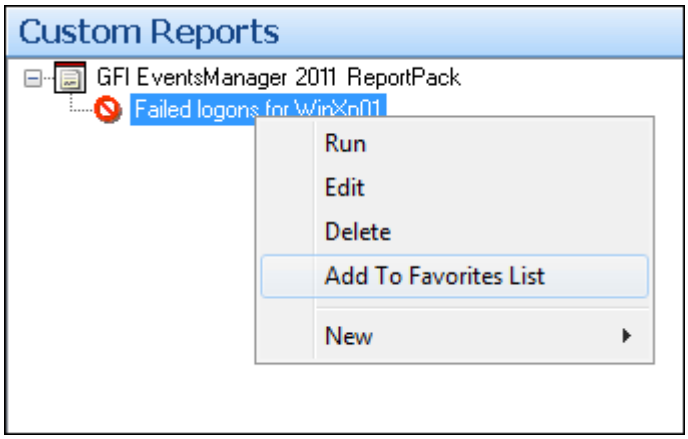
To delete a custom report:

1. Click on the **Custom Reports** navigation button.

2. Right-click on the custom report that will be permanently removed from the list and select **Delete**.

3. Click **Yes** to confirm.

4.7 Adding custom reports to the list of favorite reports



Screenshot 21 - Favorite reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a custom report to the list of favorite reports:

1. Click on the **Custom Reports** navigation button to bring up the list of available reports.

2. Right-click on the custom report that will be added to favorites and select **Add to Favorites List**.

3. Click **Yes** to confirm.

5 Scheduling reports

5.1 Introduction

GFI ReportCenter allows you to generate reports on a pre-defined schedule as well as at specified intervals. This way you can automate the generation of reports that are required on regular basis/ periodically.

Further to this, GFI ReportCenter can also be configured to automatically distribute scheduled reports via email. For every scheduled report, you can configure custom emailing parameters including the list of report recipients and the file format (e.g. PDF) the format that will be attached to the email.

Use the report-scheduling feature to automate your report generation requirements. For example, you can schedule lengthy reports after office working hours and automatically email them to the intended recipients. This way, you maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

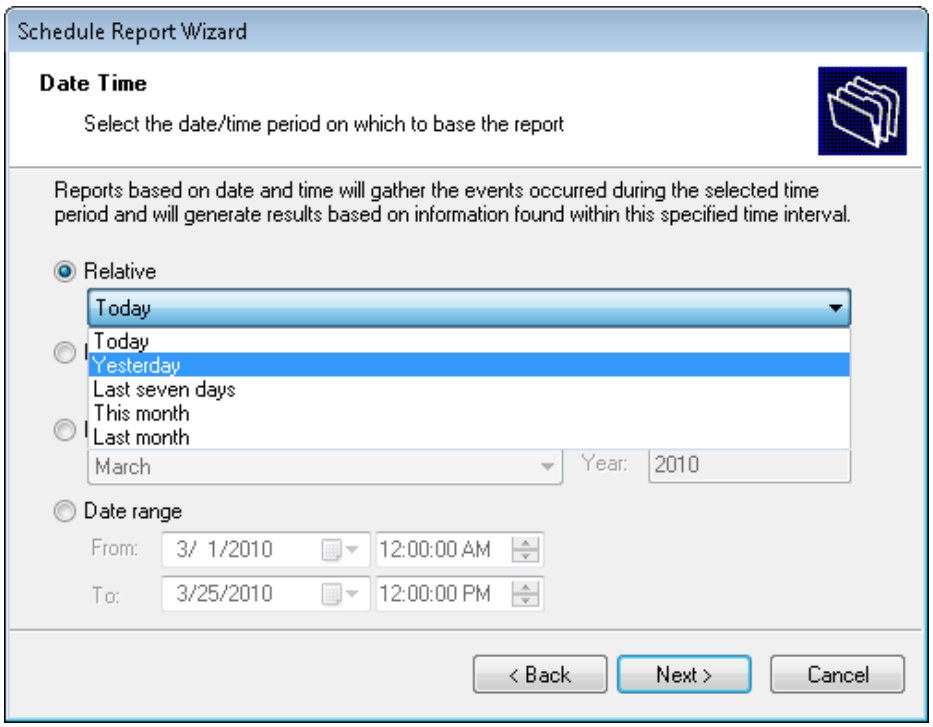
Both default and custom reports can be scheduled for automatic generation.

5.2 Scheduling a report

To schedule a report:

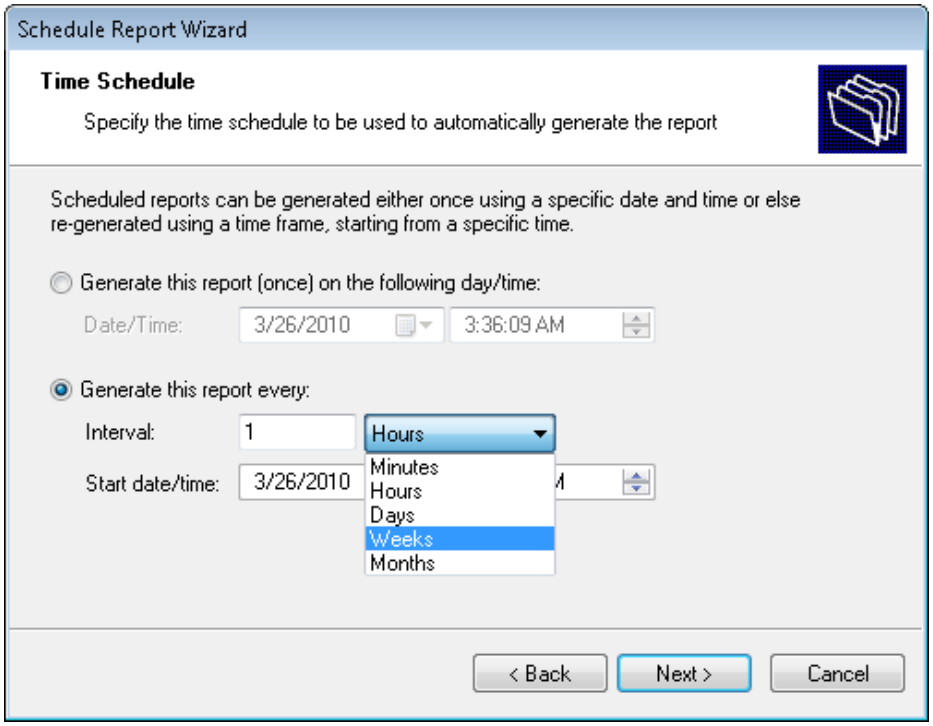
1. Click on the **Default/Custom Reports** option pane.

2. Right-click on the report to be scheduled and select **New ► Scheduled report**. To launch **Scheduled Report Wizard**. Click **Next**.



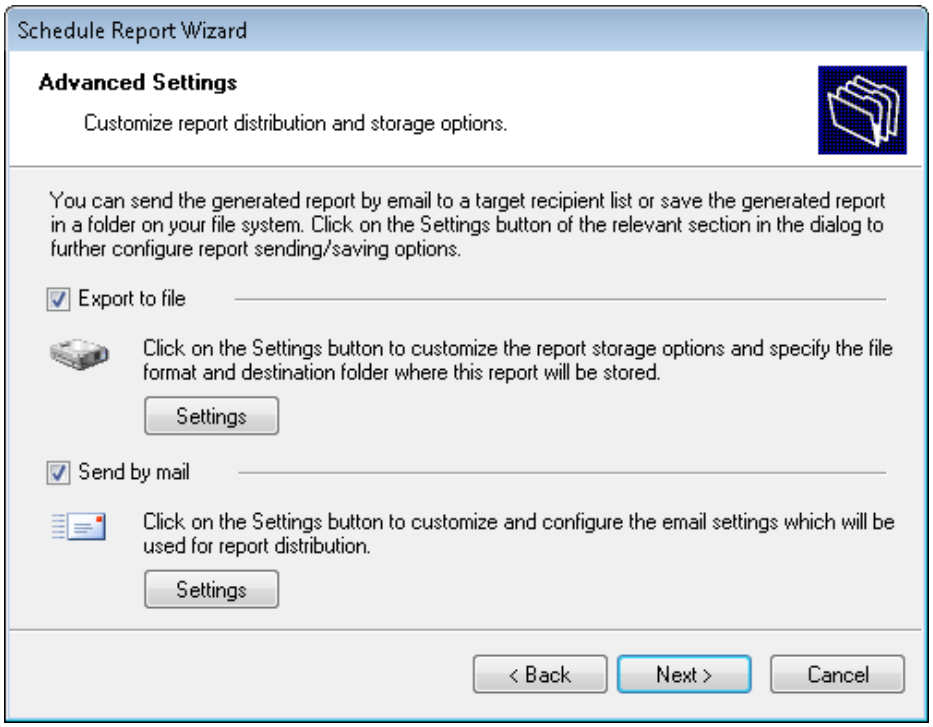
Screenshot 22 - Report Scheduling Wizard: Data-set selection dialog

3. Select the events data period to be covered by this report.



Screenshot 23 - Report Scheduling Wizard: Time schedule dialogue

4. Specify the report scheduling parameters (date/time/frequency). Click on **Next** to continue.


Schedule Report Wizard
Advanced Settings
Customize report distribution and storage options.
You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.
Export to file
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Settings
Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
Settings
< Back
Next >
Cancel

Screenshot 24 - Report Scheduling Wizard: Advanced Settings dialog

5. To export the generated report to file, select the **Export to file** option. To customize the report export configuration settings click on the **Settings** button underneath this option.

For information on how to configure, export-to-file settings refer to the 'Configuring report export to file options' section in this chapter.

6. To automatically distribute generated reports via email, select the **Send by mail** option. To customize the email settings used for report distribution click on the **Settings** button underneath this option.

For information on how to configure, email settings refer to the 'Configuring report emailing options' in this chapter.

7. Specify a name and description for this scheduled report. Click on **Next** to continue.

8. Click on **Finish** to finalize your settings.

5.3 Configuring advanced settings

GFI EventsManager ReportPack allows you to export scheduled reports to a specific file format as well as to automatically distribute these reports via email. This is achieved using either a set of parameters (e.g. recipient's email addresses) that are specified on the fly during scheduled report configuration or using the default set of report export and distribution parameters configured during the ReportPack installation.

The Report Scheduling Wizard is by default configured to use the default set of report export and distribution parameters.

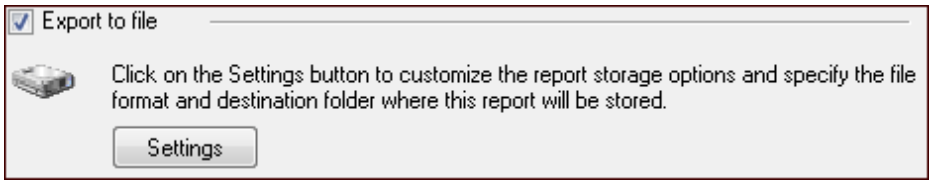
Report export formats

Scheduled reports can be exported in a variety of formats. Supported file formats include:

	Format	Description
1	Adobe Acrobat (.PDF)	Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.
2	MS Excel (.XLS)	Use this format if you want to further process the report and perform more advance calculations using another (external) program such as Microsoft Excel.
3	MS Word (.DOC)	Use this format if you want to access this report using Microsoft Word.
4	Rich text format (.RTF)	Use this format to save the report in a format that is small and that allows accessibility through different word processors in different operating systems.

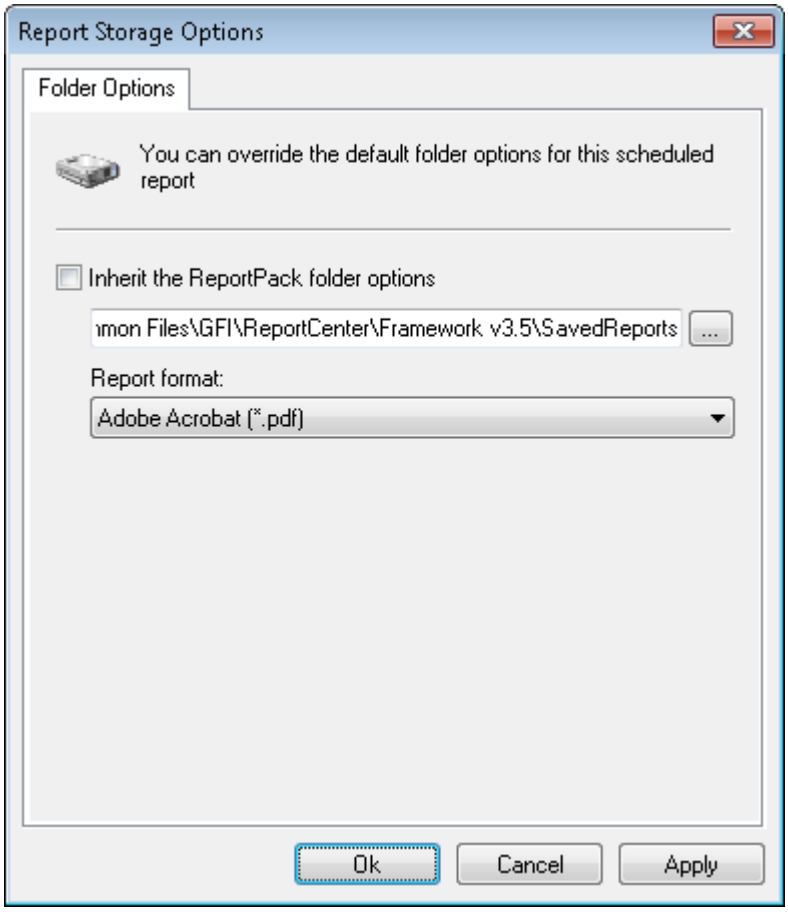
5.3.1 Configuring report export to file options

To configure the report export settings do the following:


Export to file
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Settings

Screenshot 25 - Advanced Settings dialog: Export to file settings button

1. From the **Advanced Settings** dialog, click on the **Settings** button underneath the **Export to file** option.



Screenshot 26 - Advanced Settings: Export to file options

2. Un-check the option **Inherit the ReportPack …**

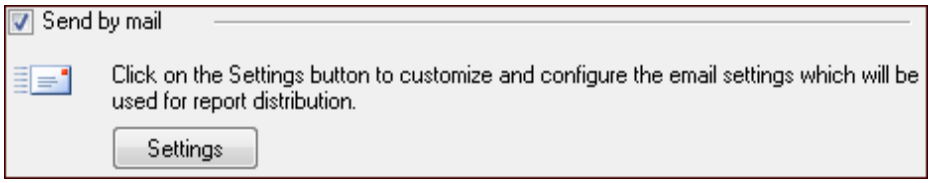
3. Specify the complete path were the exported report will be saved.

4. Specify the exported file format.

5. Click **OK** to finalize your configuration settings.

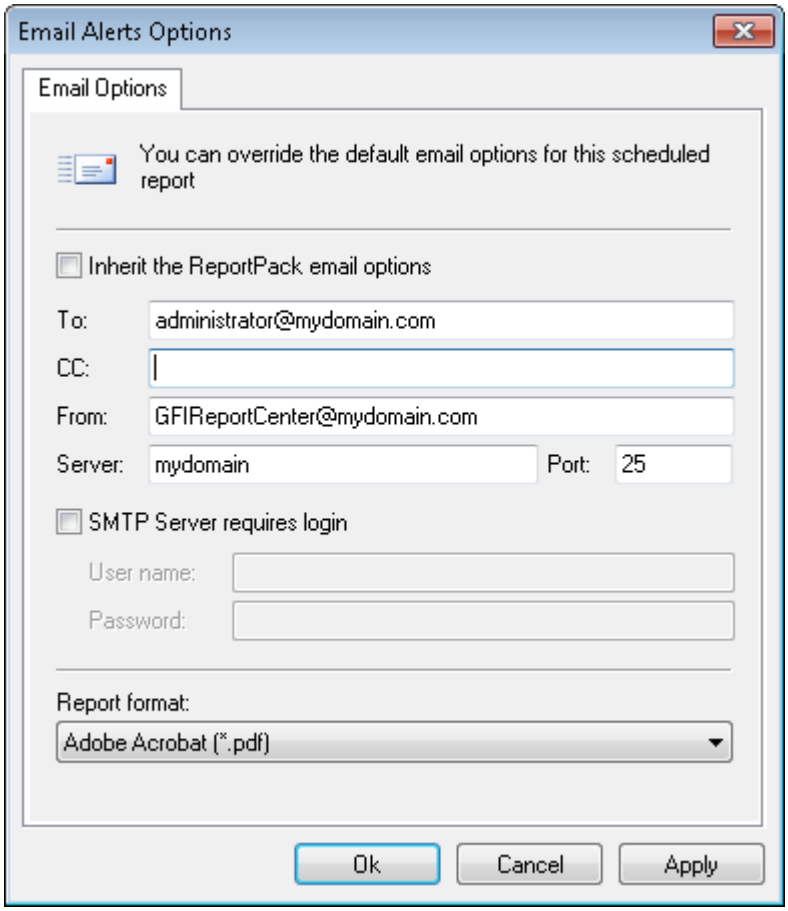
5.3.2 Configuring report emailing options

To configure the report emailing options of a scheduled report do as follows:


Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
Settings

Screenshot 27 - Advanced Settings dialog: Send by email settings button

1. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the **Send by email** option.



Screenshot 28 - Report distribution options

2. Un-Check the option, **Inherit the ReportPack…**

3. Specify the following parameters:

» **To/CC**: Specify the email address(es) were the generated report will be sent.

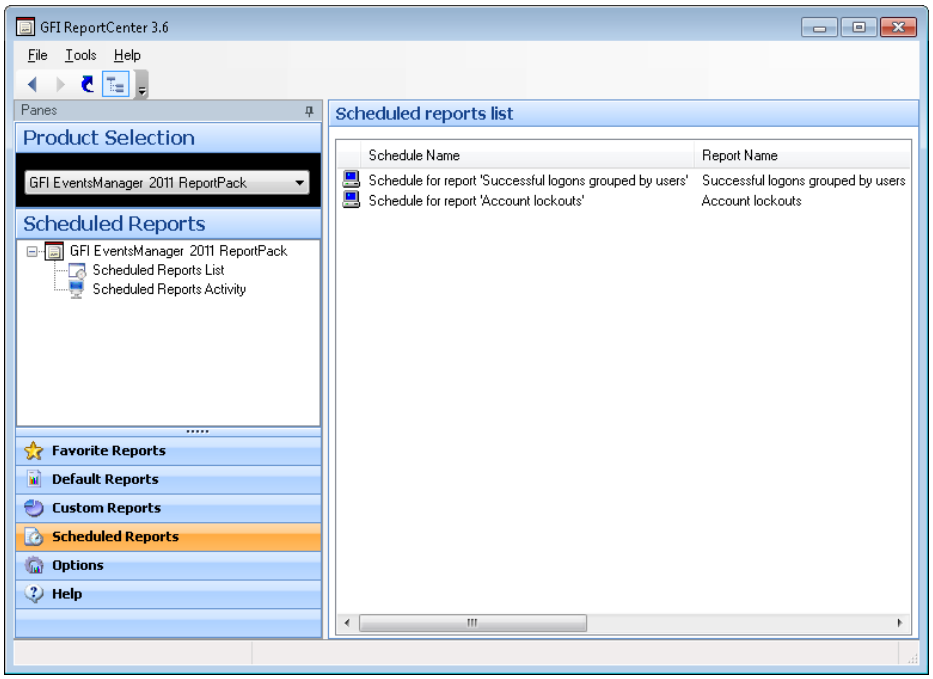
» **From**: Specify the email account that will be used to send the report.

» **Server**: Specify the name/IP of your SMTP (outbound) email server. If the specified server requires authentication, select the option 'SMTP Server requires login' and specify the logon credentials in the **User name** and **Password** fields.

» **Report format**: Reports are sent via email as attachments. Select the report file format.

4. Click **OK** to finalize your configuration settings.

5.4 Viewing the list of scheduled reports

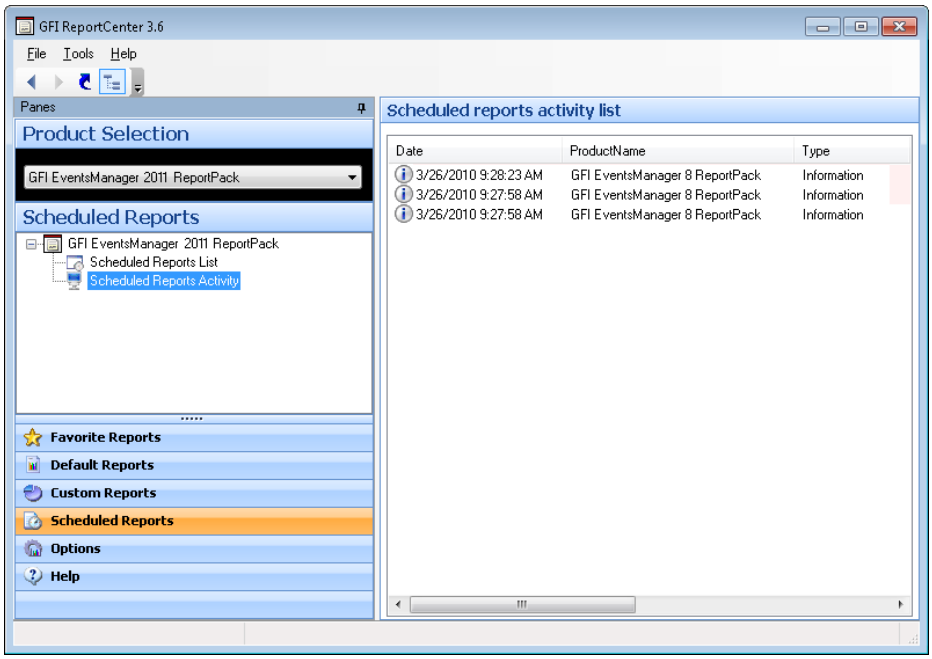


Screenshot 29 - List of Scheduled reports

Click on the **Scheduled Reports** navigation button to show the list of scheduled reports that are currently configured for automatic generation. This information is displayed in the right pane of the management console and includes the following details:

- **Schedule Name:** The custom name that was specified during the creation of the new scheduled report.
- **Report Name:** The names of the default or custom report(s) that will be generate.
- **Last Generation:** Indicates the date/time when the report was last generated.
- **Next Generation:** Indicate the date/time when the report is to be next generated.
- **Description**: The description that you have entered for each schedule.

5.5 Viewing the scheduled reports activity



Screenshot 30 - Schedule activity monitor

GFI ReportCenter also includes a schedule activity that enables you to monitor the events related to all scheduled reports that have been executed.

To open the schedule activity monitor, click on the **Scheduled Reports** navigation button and select the **Scheduled Reports Activity** node. This will bring up the activity information in the right pane of the GFI ReportCenter management console.

The activity monitor displays the following events:

» **Information**: The scheduled report was successfully executed and sent by email and/or saved to disk.

» **Warning**: The scheduled report was not executed because product license is invalid or has expired.

» **Error**: The scheduled report was not executed due to a particular condition/event. Typical conditions include:

- Errors when attempting to save the generated report to a specific folder (for example, out of disk space).
- Errors when attempting to send the generated report via email (for example, the SMTP server configured in the GFI ReportCenter settings is not reachable).

The activity monitor records and enumerates the following information:

» **Date:** The date and time when the scheduled report was executed.

» **Product name**: The name of the GFI product that the report belongs.

» **Type:** The event classification - error, information, or warning.

» **Description:** Information related to the state of a scheduled report that has been executed. The format and contents of the activity description vary, depending on the event type.

The description is often the most useful piece of information, indicating what happened during the execution of a scheduled report or the significance of the event.

5.6 Enable/disable a scheduled report

Scheduled reports can be enabled or disabled as required. Use the **Scheduled Reports** navigation button to view the list of scheduled reports as well as to identify their status. The status of scheduled reports is shown through the icon included on the left hand side of each schedule:

- Indicates that the scheduled report is disabled.

- Indicates that the scheduled report is enabled/pending.

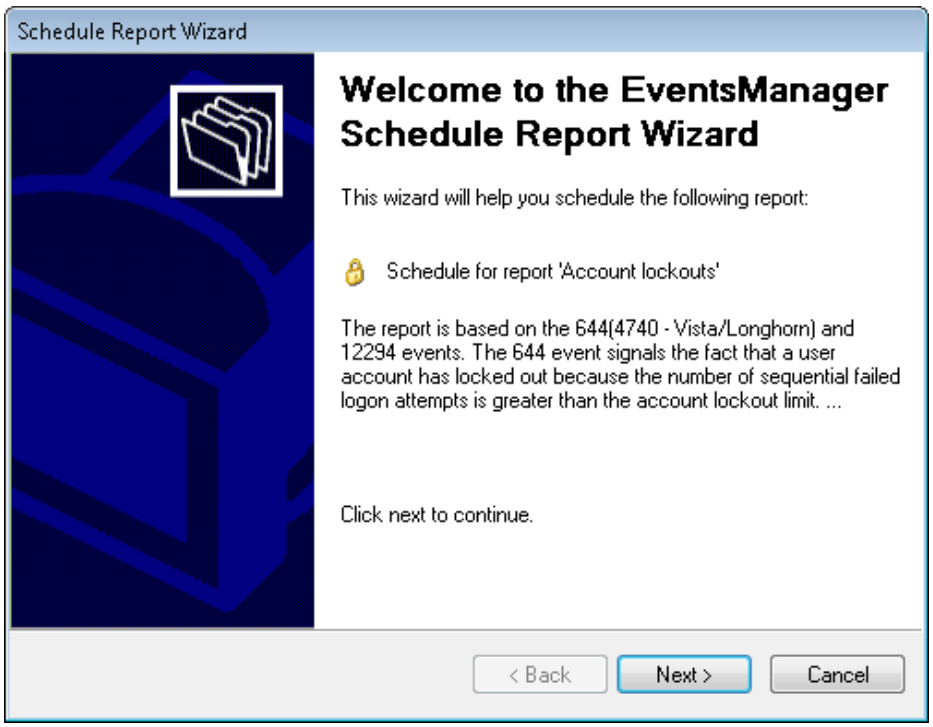
To enable or disable a scheduled report, right-click on the respective report and select **Enable/Disable** accordingly.

5.7 Editing a scheduled report

To make changes to the configuration settings of a scheduled report:

1. Click on the **Scheduled Reports** navigation button.

2. Right-click on the scheduled report to be re-configured and select **Properties**. This will bring up the **Scheduled Reports Wizard**.


Schedule Report Wizard
Welcome to the EventsManager Schedule Report Wizard
This wizard will help you schedule the following report:
Schedule for report 'Account lockouts'
The report is based on the 644(4740 - Vista/Longhorn) and 12294 events. The 644 event signals the fact that a user account has locked out because the number of sequential failed logon attempts is greater than the account lockout limit. ...
Click next to continue.
< Back
Next >
Cancel

Screenshot 31 - Scheduled Reports wizard

3. Click on **Next** and perform the required changes. For information on how to configure the parameters of a scheduled report refer to the Scheduling a report section in this manual.

5.8 Deleting a scheduled report

To delete a scheduled report:

1. Click on the **Scheduled Reports** navigation button.

2. Right-click on the scheduled report and select **Delete**.

5.9 Example: Scheduling a report

This example demonstrates how to schedule a failed logons report that will:

» Generate the first report on 01/04/2010 at 20:00.

» Continue generating the same report on a daily basis.

» Export the generated report(s) to folder **C:\Daily Reports** in PDF format.

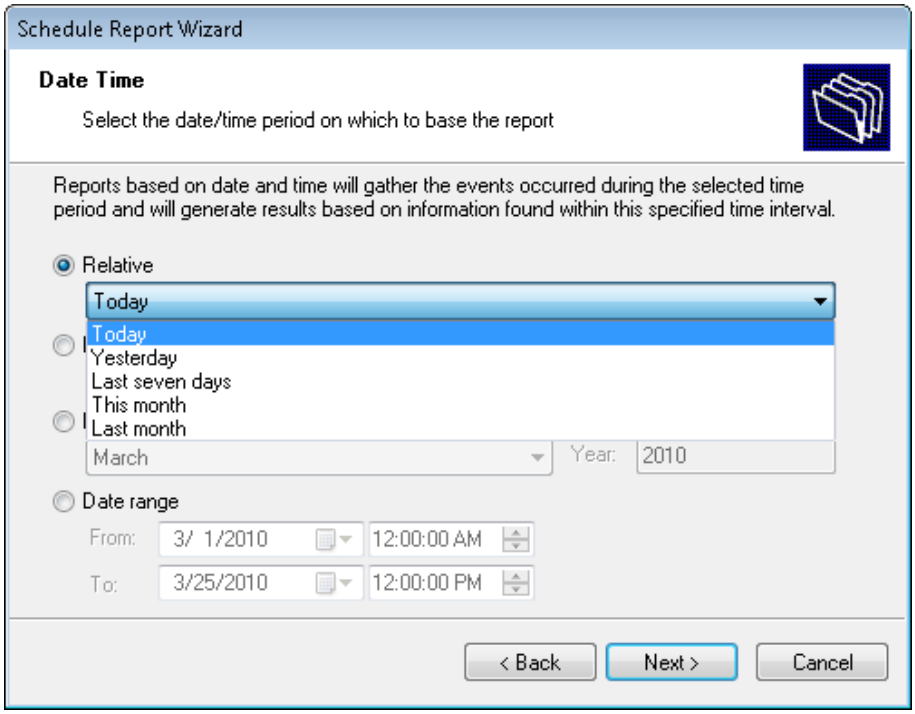
» Email the generated report using the following custom parameters:

- Send from email account: **GFIReportCentre@mydomain.com**
- Send to email account: **administrator@mydomain.com**
- SMTP server details: **mydomain**

To create the scheduled report:

1. Click on the **Default Reports** navigation button.

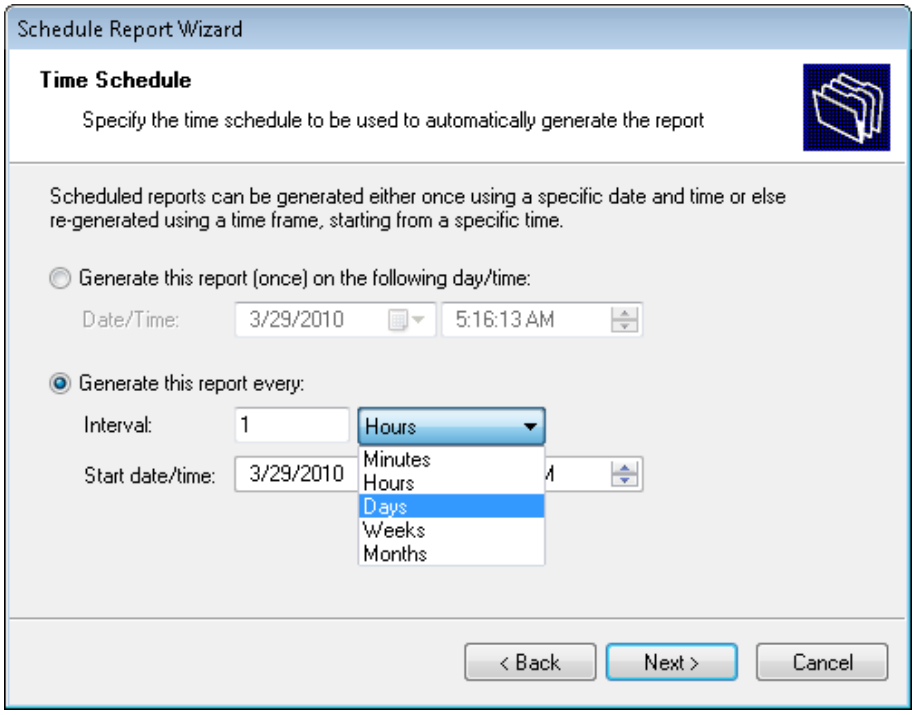
2. Right-click on **Failed logons** and select **New ► Scheduled Report**, click **Next**.



Screenshot 32 - Select events data period

3. Select the option **Relative** and from the provided drop down list select **Today**. Click on **Next** to proceed to the next dialog.

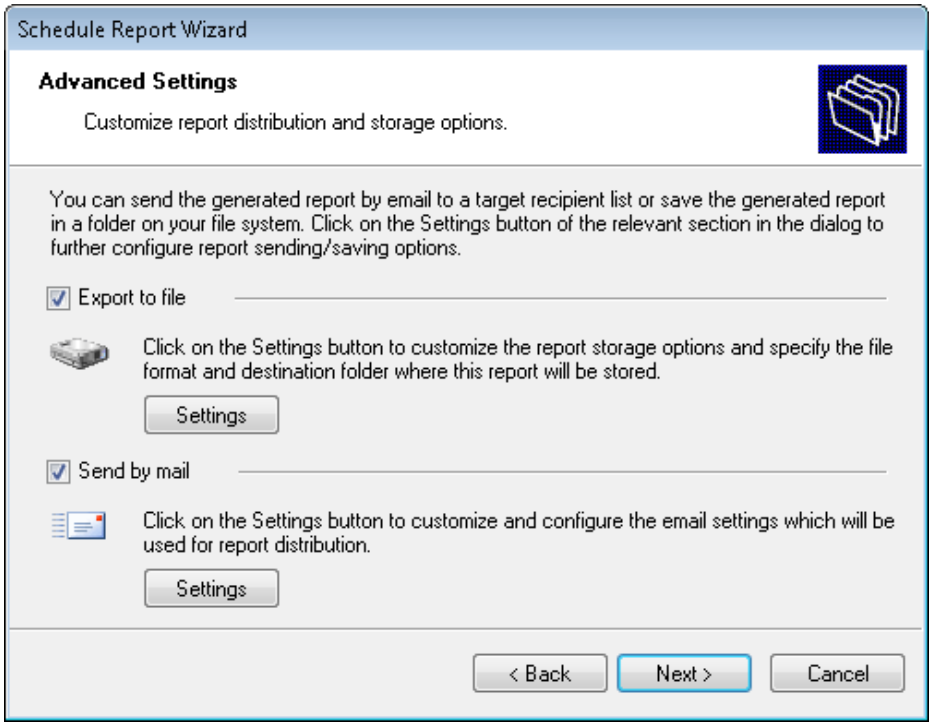
4. Since no data filters will be applied in this example, click **Next** to proceed to the next dialog.



Screenshot 33 - Specifying the scheduling options

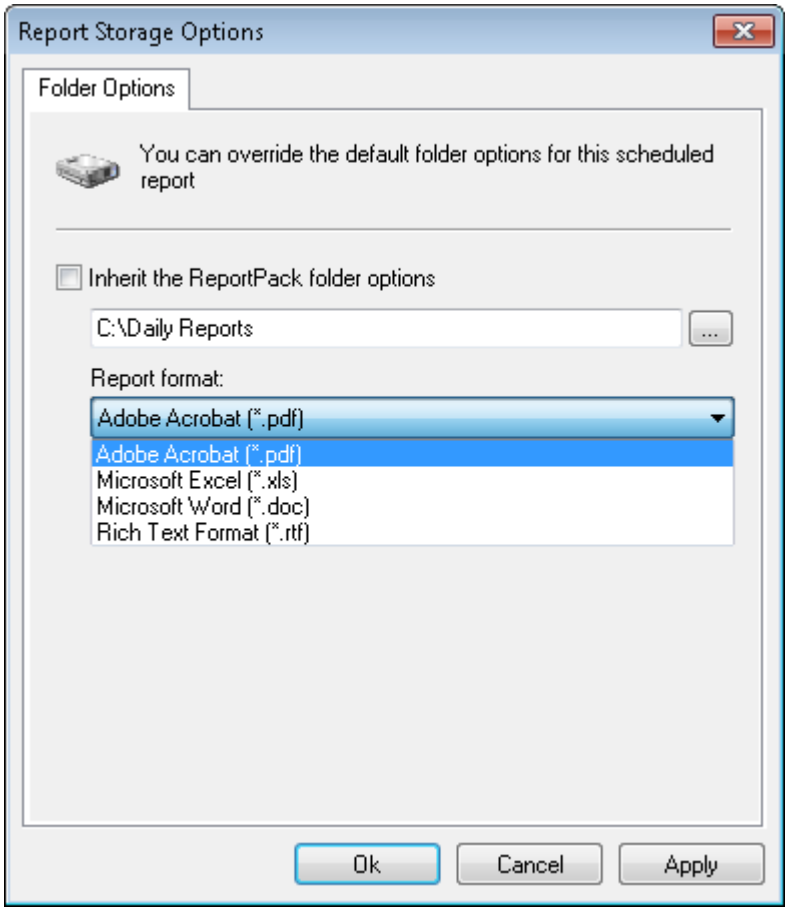
5. To generate this report on daily basis, select the option **Generate this report every:** and set the interval to **1 Day**.

6. Set the start date to **01/04/2010** and time to **20:00**. Click **Next** to continue.


Schedule Report Wizard
Advanced Settings
Customize report distribution and storage options.
You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.
Export to file
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Settings
Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
Settings
< Back
Next >
Cancel

Screenshot 34 - Advanced Settings dialog

7. From the **Advanced Settings** dialog, click on the **Settings** button underneath the **Export to file** option.

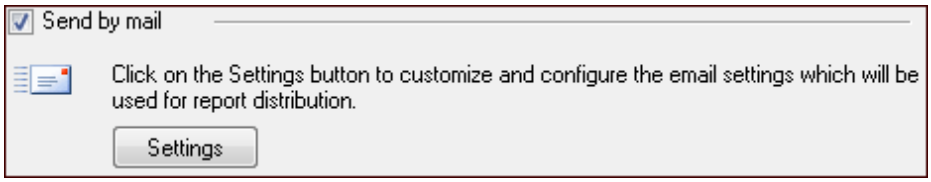


Screenshot 35 - Advanced Settings: Export to file options

8. Un-check the option **Inherit the ReportPack folder options:**

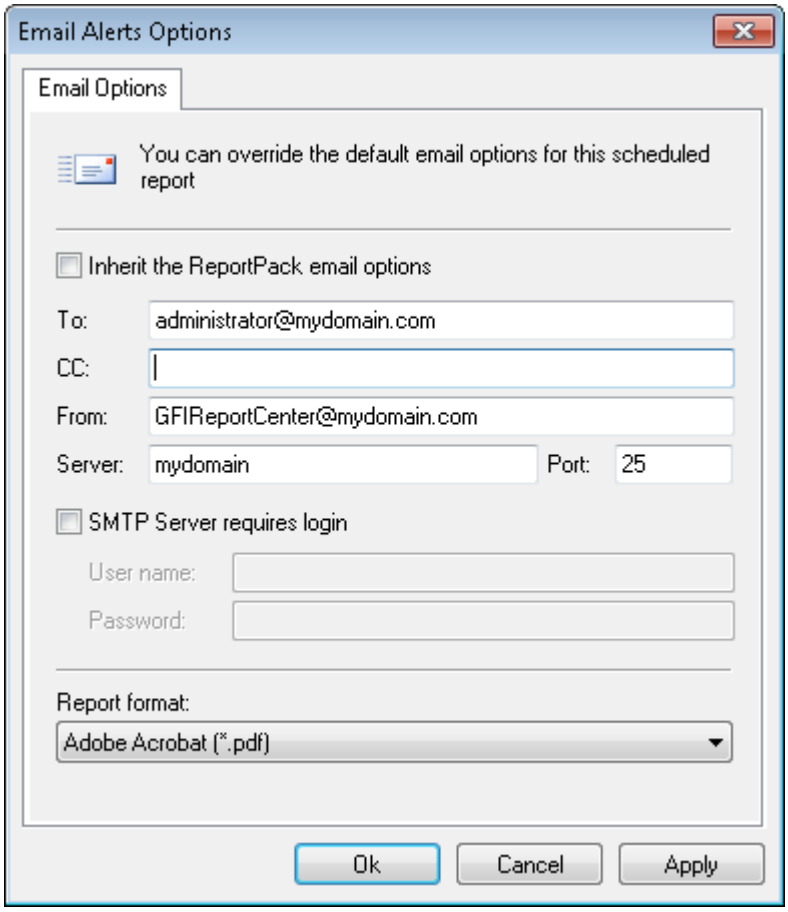
9. Specify the complete path were this report will be saved i.e. **C:\Daily Reports.**

10. From the report format drop down select **PDF** and click **OK**.


Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
Settings

Screenshot 36 - Advanced Settings dialog: Send by email settings button

11. From the **Advanced Settings** dialog, click on the **Settings** button underneath the **Send by email** option.



Screenshot 37 - Report distribution options

12. Un-check the option **Inherit the ReportPack email options**:

13. Specify the following parameters:

» **To:** administrator@mydomain.com

» **From:** GFIReportCenter@mydomain.com

» **Server:** mydomain

14. From the report format drop down select **PDF** and click **OK** to finalize your email settings.

15. Click **Next** and specify the following parameters:

» **Report Name**: Daily failed logons report

» **Report Title**: Daily failed logons report

» **Report Description**: This report is generated on a daily basis at 20:00. It shows all failed logon events recorded throughout the day.

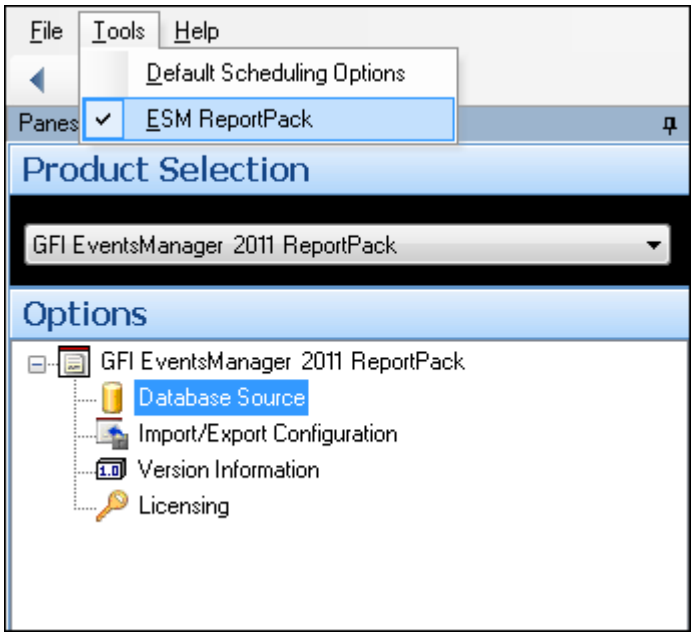
16. Click **Next** to proceed to the final dialog.

17. Click **Finish** to finalize your custom report configuration settings.

6 Configuring default options

6.1 Introduction

The GFI EventsManager ReportPack allows you to configure a default set of parameters that can be used when generating reports. These parameters are first set during installation. However, you can still reconfigure any of these parameters via the **Options** navigation button and the **Tools** menu provided in the GFI ReportCenter management console.



Screenshot 38 - Options navigation button and Tools menu

Through the **Options** navigation button, you can configure the following parameter:

» **Database source:** Use this node to specify the database backend from were the ReportPack will extract the required reporting data.

Through the **Tools** menu, you can configure the following parameters:

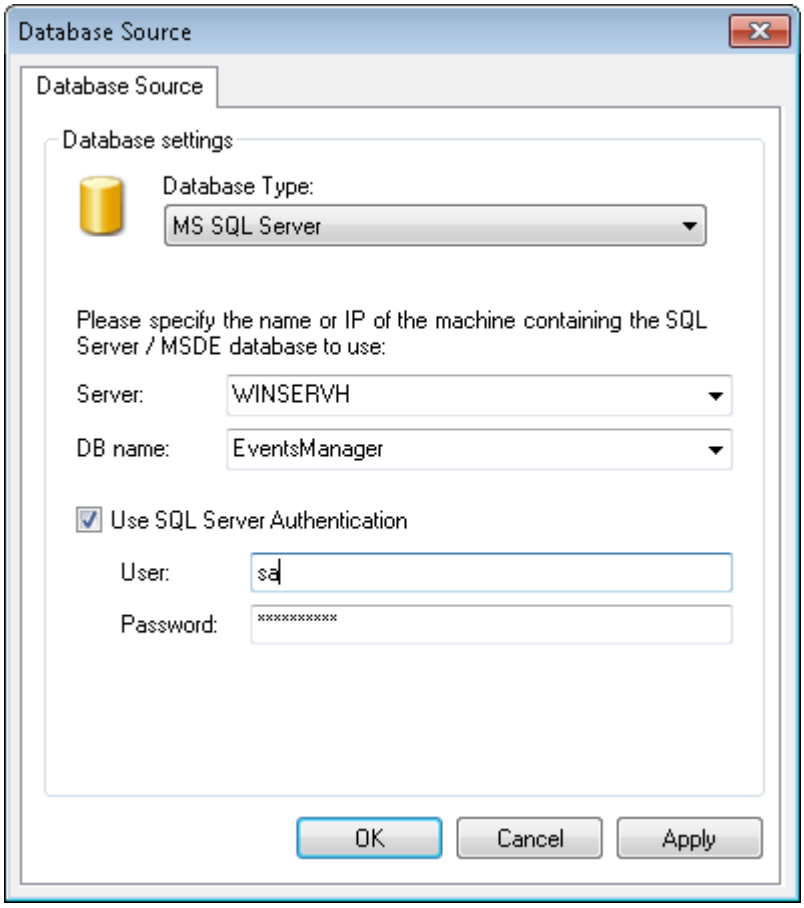
» **Default scheduling settings:** Use this menu option to configure the default export to file parameters and report emailing parameters of scheduled reports.

6.2 Configuring database source

To configure your database source:

1. Click on the **Options** navigation button.

2. Right-click on the **Database Source** node and select **Set Database Source…** This will bring up the database source configuration dialog.



Screenshot 39 - Database source configuration dialog

3. Select the database type (e.g. MS SQL Server) from the provided list of supported databases.

GFI EventsManager database backend supports only MSDE/MS SQL Server.

4. Specify the name or IP address of your MSDE/MS SQL Server database backend.

5. To use the credentials of an SQL Server account, select the **Use SQL Server authentication** option and specify the user name and password in the provided fields.

By default, the GFI EventsManager ReportPack uses Windows logon credentials to authenticate to the SQL Server.

6. Specify the name of the database to be used by the database backend.

7. Click on **OK** to finalize your configuration settings.

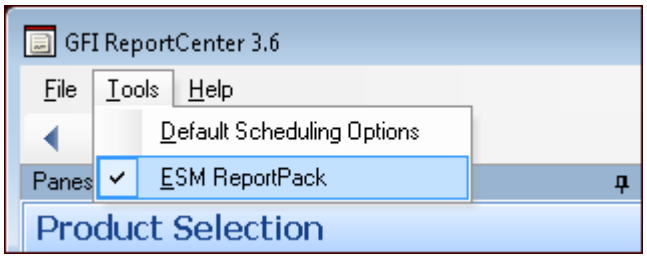
6.3 Viewing the current database source settings

Screenshot 40 - Database source configuration settings

After configuration, you can view the current database source settings by clicking on the **Database Source** node.

6.4 Configuring default scheduling settings

To configure the default settings to be used by scheduled reports:



Screenshot 41 - Default Scheduling Options node

1. From the pull-down menu, click on the **Tools ► Default Scheduling Options**.

2. Configuration the required parameter as described in the Configuring advanced settings in this manual.

7 Exporting and Importing Configuration

7.1 Introduction

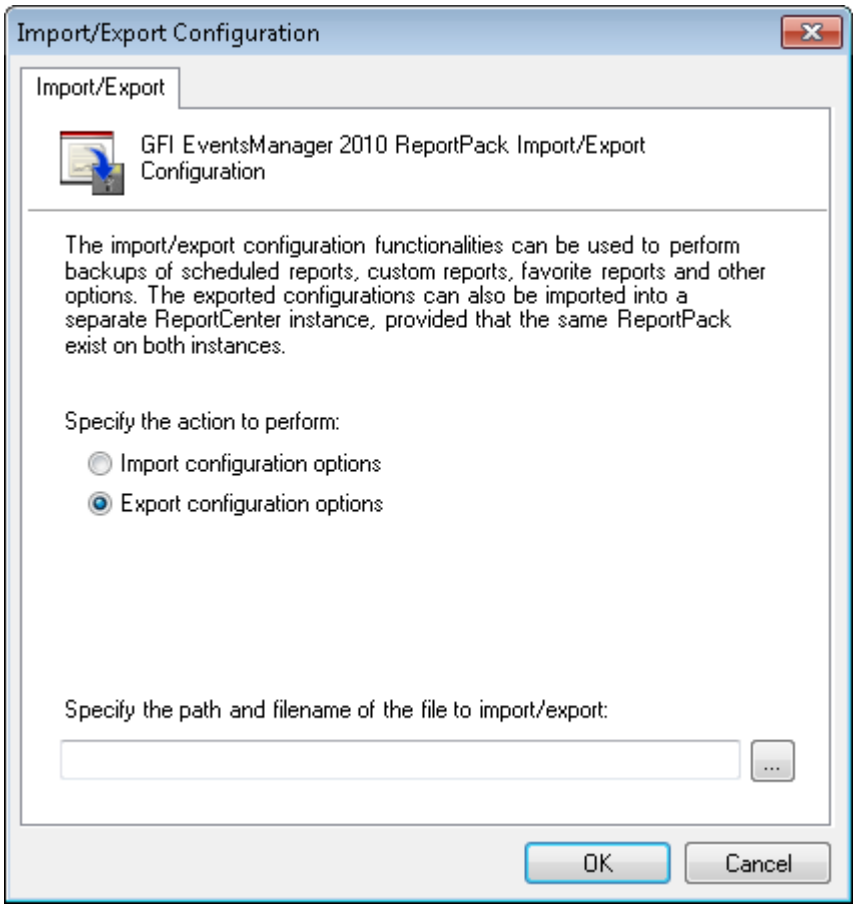
This section contains information on how to import and export GFI EventsManager ReportPack settings. The Import/Export feature enables you to take a backup of the custom and scheduled reports. This feature is also useful if you need to import settings on a separate installation of GFI ReportCenter.

7.2 Exporting settings

To export all settings:

1. Click **Options** panel button.

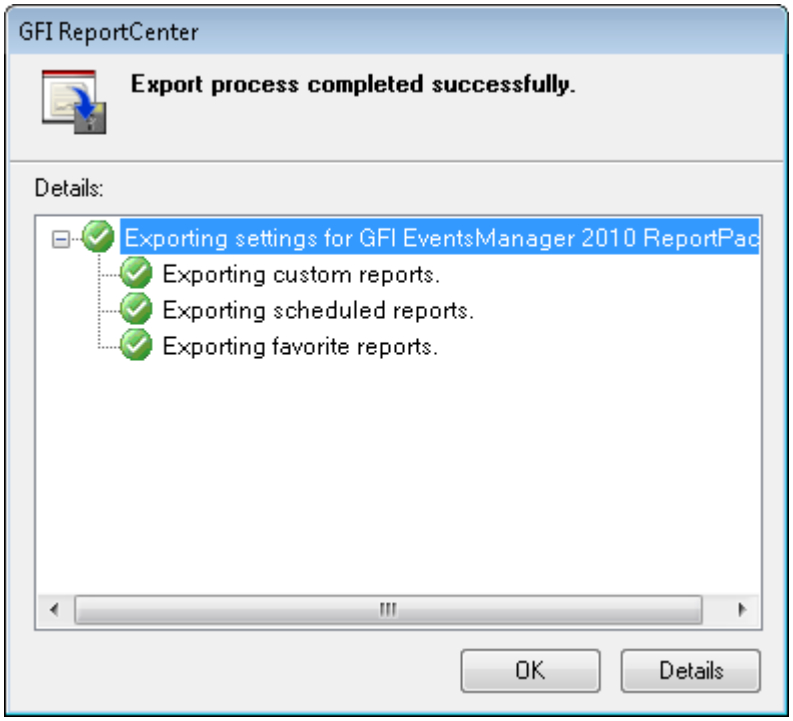
2. Right-click **Import/Export Configuration** node and select **Import/Export Configuration**.


Import/Export Configuration
Import/Export
GFI EventsManager 2010 ReportPack Import/Export Configuration
The import/export configuration functionalities can be used to perform backups of scheduled reports, custom reports, favorite reports and other options. The exported configurations can also be imported into a separate ReportCenter instance, provided that the same ReportPack exist on both instances.
Specify the action to perform:
Import configuration options
Export configuration options
Specify the path and filename of the file to import/export:
...
OK
Cancel

Screenshot 42 - Export setting dialog box

3. Click **Export configuration options**.

4. Browse and select the path where to export settings and click **OK**.



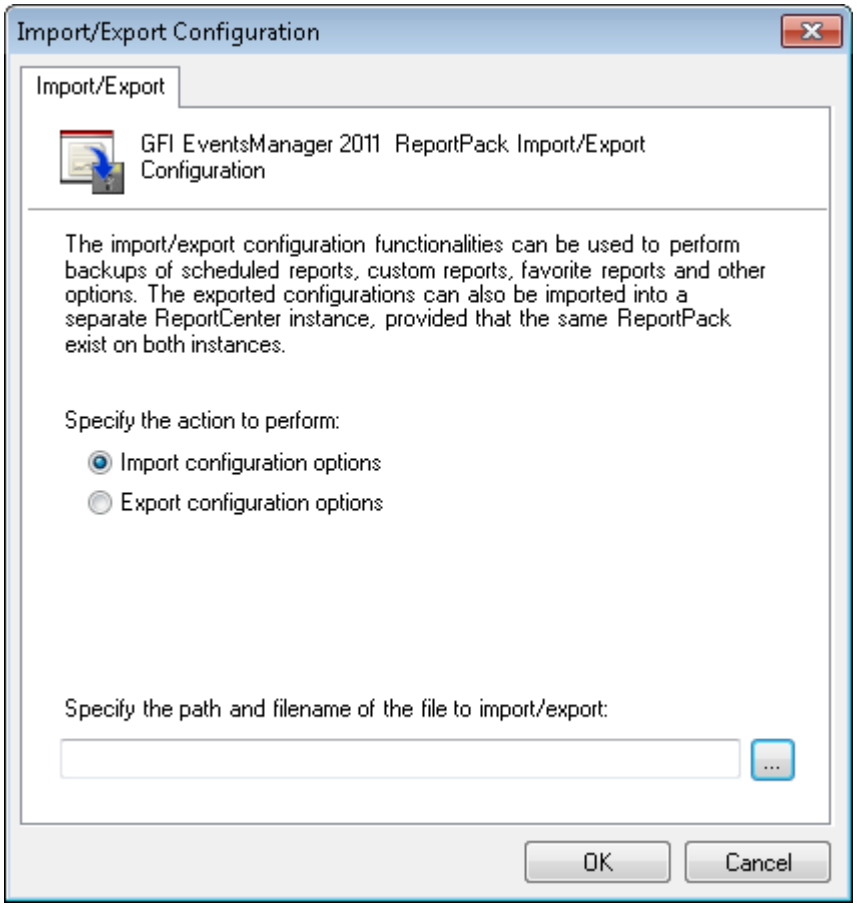
Screenshot 43 - Settings exported successfully

5. Click **OK**.

7.3 Importing settings

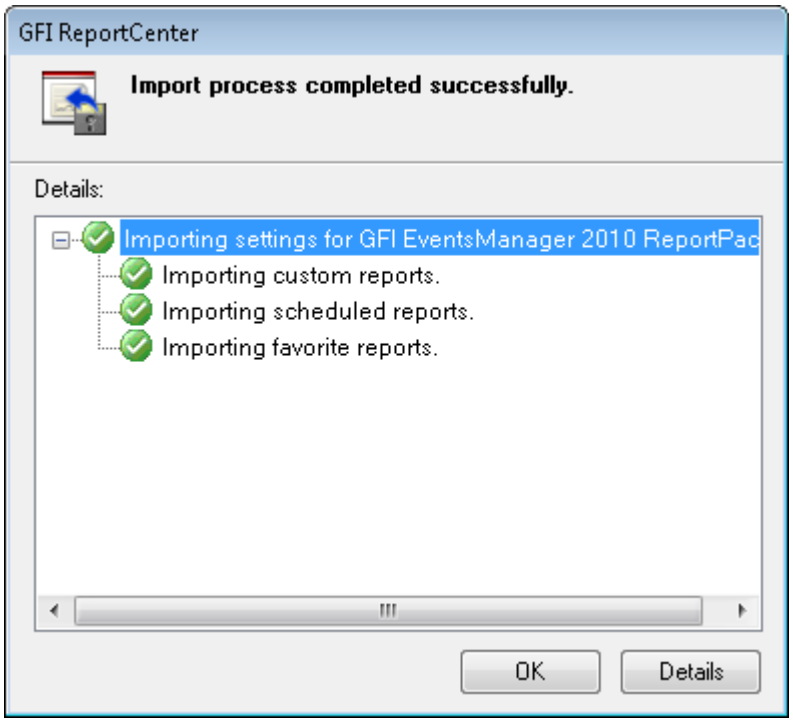
To import GFI EventsManager ReportPack settings:

1. Click **Options** panel button.
2. Right-click **Import/Export Configuration** node and select **Import/Export Configuration**.
3. Click **Import configuration options**.


Import/Export Configuration
Import/Export
GFI EventsManager 2011 ReportPack Import/Export Configuration
The import/export configuration functionalities can be used to perform backups of scheduled reports, custom reports, favorite reports and other options. The exported configurations can also be imported into a separate ReportCenter instance, provided that the same ReportPack exist on both instances.
Specify the action to perform:
Import configuration options
Export configuration options
Specify the path and filename of the file to import/export:
...
OK
Cancel

Screenshot 44 - Import setting dialog box

4. Browse and locate the exported settings (XML format). Click **OK**.



Screenshot 45 - Settings imported successfully

5. Click **OK** when the process completes.

Restart GFI EventsManager ReportPack to apply imported settings.

8 General options

8.1 Entering your license key after installation

If you have purchased GFI EventsManager, enter your License key using the **Options** ► **Licensing** node (no re-installation/re-configuration required)

Entering the License Key should not be confused with the process of registering your company details on our website. This is important since it allows us to give you support and notify you of important product news. You may register and obtain your GFI customer account from: http://www.gfi.com/pages/regfrm.htm.

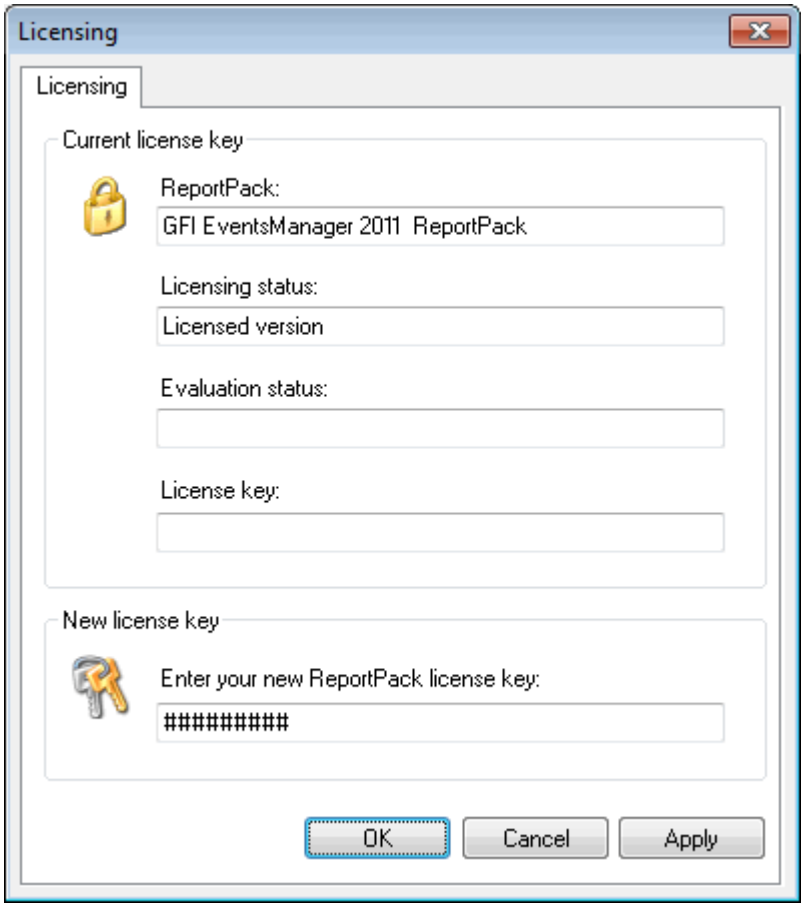
To input your GFI EventsManager license key:

Screenshot 46 - Product Selection drop down list

1. Select the respective product (e.g. GFI EventsManager 8 ReportPack) from the **Product Selection** drop down list.

2. Click on the **Options** navigation button.

3. Right-click on the **Licensing** node and select **Set Licensing**…



Screenshot 47 - Licensing dialog

4. Type in the GFI EventsManager license key.

5. Click on **OK** to finalize your entry.

8.2 Viewing the current licensing details

To view your current licensing details, click on the **Options** navigation button and select the **Licensing** node. The licensing details will be displayed in the right pane of the management console.

8.3 Viewing the product ReportPack version details

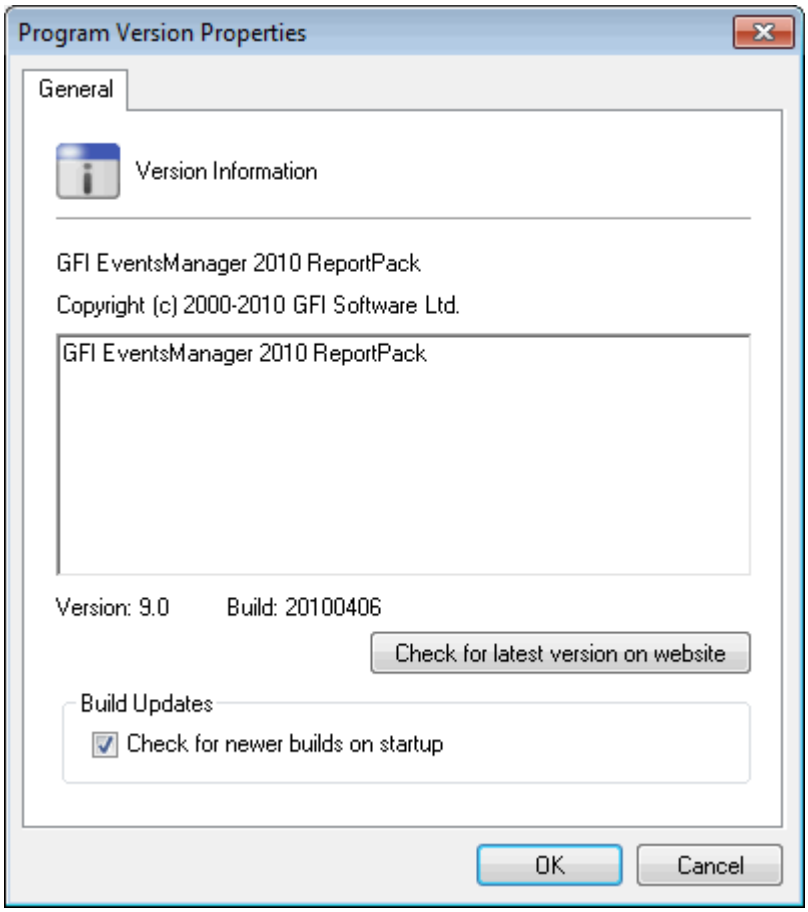
To view the version information of your product ReportPacks:

1. Select the product ReportPack from the **Product Selection** drop down list.

2. Click on the **Options** navigation button and select the **Version Information** node. The version details will be displayed in the right pane of the management console.

8.4 Checking the web for newer builds

Periodically GFI releases product and ReportPack updates that can be automatically downloaded from the GFI website. To check if a newer built is available for download:



Screenshot 48 - Version Properties: Check for newer builds dialog

1. Select the respective product (for example, GFI EventsManager 8 ReportPack) from the **Product Selection** drop down list.

2. Click on the **Options** navigation button.

3. Right-click on the **Version Information** node and select **Checking for newer builds…**

9 Appendix: Default Reports

9.1 Introduction

This section contains a short description of each report that can be generated using GFI EventsManager ReportPack.

9.2 Account Usage Reports

Report name	Description
Successful logons grouped by users	This report is based on event 528 (4624 - Vista/Longhorn) - successful logon and event 540 (4636 - Vista/Longhorn) - successful network logon. This report enables you to monitor all successful logons on your network grouped by user name and helps achieve compliance with legal acts that require monitoring of company resources.
Successful logons grouped by computers	This report is based on event 528 (4624 - Vista/Longhorn) - successful logon and event 540 (4636 - Vista/Longhorn) - successful network logon. This report enables you to monitor all successful logons on your network grouped by computers and helps achieve compliance with legal acts that require monitoring of company resources.
Failed logons	This report is based on events 529 to 535 (4625 - Vista/Longhorn) and event 675 (4771 - Vista/Longhorn). This report shows all login failures including the failure cause. Amongst others, this report helps to investigate multiple logon failures that are below the account lockout threshold and attempted abuse by contractors and former internal users.
Logoff events	This report is based on event 538 (4634 - Vista/Longhorn) - user logoff. The report shows all logoff events and includes the logon type field. Compare the logoff events with the successful logon events to determine the duration of each user session.
Account logons	This report shows the logon attempts on domain controllers. This report shows all NTLM logon attempts, Kerberos authentication and service tickets requests, Kerberos failed events and terminal services account logon events.
Account lockouts	This report is based on event 644 (4740 - Vista/Longhorn) and event 12294 events. The 644 event indicates a locked user account when the number of sequential failed logon attempts exceeded the lockout limit. The 12294 event indicates a possible brute force attack trying to break the default Administrator account. Since this account does not lock out, the system event logs records SAM event 12294.
Successful logon count on each computer	The report collects information on successful logon events and provides a quick view of the most accessed computers / domain in the network.
Failed logon count on each computer	The report is based on the failed logon events and provides a quick view of the login errors occurred on each computer.
Top 10 accounts which failed to logon	The report is based on the failed logon events and provides a quick view of the most frequent login errors occurred on each computer.
Accounts which Failed Logon	The report is based on the failed logon events that occurred on each computer.

9.3 Account Management

Report name	Description
User account management	This report enables you to monitor, irregular or unusual network account activities. Amongst others, this report helps you to identify potential abuse using administrators' privileges.
Computer account management	Computers running Windows NT, Windows 2000, Windows XP, Windows Vista or Windows Server 2003/2008 that are members of a domain, have an associated computer domain account. This report shows the auditing of computer access to the network and to domain resources as well as information about the domain members.
Password changes	This report enables you to monitor; password operation events, change password attempts and changes to the directory service when the account is a domain member.
Security group management	Good security practice advocates the principle of least privilege, which translates into giving users the minimum rights and permissions they need to do their jobs. Most user accounts should be members of the Domain Users group only, together with any organization-specific security groups. Assigning Domain, Schema or Enterprise Admins privilege to users must occur within policy guidelines only, and should make use of established and approved accounts or processes. You should treat any other changes as suspicious and investigate further.

9.4 Policy Changes

Report name	Description
Local audit User right assignment policy changes	The report is based on event 612 (4719 - Vista/Longhorn) - local audit policy changed. The event identifies any changes to the audit policy. Compare these events with changes that authorized personnel did to audit policy.
Domain policy changes	The report is based on event 643 (4739 - Vista/Longhorn) - domain policy changed. The event identifies any changes to the domain audit policy. Compare these events with changes that authorized personnel did to audit policy.
User right assignment policy changes	The report is based on events 608 (4704 - Vista/Longhorn) and 609 (4705 - Vista/Longhorn). The report shows when a new privilege is granted/removed to/from a user account. The event log records these actions with the user account Security Identifier (SID). In order to display the information in a more understandable manner, the privileges granted are translated to the associated policy name that was changed. For example, instead of SeTcbPrivilege, the report lists "Act as part of the operating system".
System access granted/removed	The report is based on events 621 (4717 - Vista /Longhorn) and 622 (4718 - Vista/Longhorn). The events records when a user was granted access to a system or user system access was removed. Check User Name and Account Modified, particularly if access permission is interactive. Event 622 might indicate that an attacker removed evidence of event 621 (system access granted to user account) in order to cover the trails, or is attempting to deny service to some other account(s).
Encrypted Data Recovery policy	The report is based on event 618 (4714 - Vista/Longhorn). If encrypted data recovery policy is in use, monitor for this event and investigate any occurrences outside specified policy.
IPSEC policy changes	This report is based on events 613 (4709 - Vista/Longhorn), 614 (4710 - Vista/Longhorn) and 615 (4711 - Vista/Longhorn). Monitor these events and investigate any occurrences that are outside system startups.
Kerberos policy changes	This section is based on event 617 (4713 - Vista/Longhorn). The event signals a Kerberos policy change. Verify if the user performing the change is authorized and if the change occurs according to your security policies/plans.

9.5 Object Access

Report name	Description
Failed attempts to access files and registry	This report is based on event 560 (4656 - Vista/Longhorn) with type failure audit. These events show when an object has rejected access to a request, such as list, read, create, and delete. This report shows failed attempts to access files or registry and does not include normal system activity. Note that for best results, file auditing is required to be enabled on the files and registry values of interest. Use This report to identify users who are trying to access resources they are not granted access to.
Successful attempts to access files and registry	This report is based on event 560 (4656 - Vista/Longhorn) with type success audit. These events show were an object has granted access to a request, such as list, read, create, and delete. This report shows successful attempts to access files or registry and does not include normal system activity. Note that for best results, file auditing is required to be enabled on the files and registry values of interest. Use This report to identify the users accessing sensitive information.
Object deleted with details	This report is based on events 564 (4660 - Vista/Longhorn) - object deleted and 560 (4656 - Vista). Use this report to view the users deleting objects like files, registry, printers, etc.

9.6 Application Management

Report name	Description
Applications installed/removed	This report shows events from the application log with source "MsiInstaller". It displays the applications successfully installed/uninstalled using Windows Installer technology, and failed attempts to install or uninstall applications.
Applications crashing or hanging	This report shows events from the application log with sources "Application Error", "Application Hang" and "DrWatson". This report displays all the applications that crashed or hanged, together with the associated information.

9.7 Print Server

Report name	Description
Print activities	This report shows events 2-14 from the system log, with source "print". It displays all the documents printed, the users printing documents, the file details of the printed files and the date and time when the print operation took place.

9.8 Windows Event Log system

Report name	Description
Event Log health	This report shows important events from the system log, with source EventLog. It displays events like log full, log file corrupt, Event Log service stopping /starting, and unexpected system shutdowns. Use this report to determine failures in the auditing process. These failures may be exploited by attackers and usually lead to loss of audit entries. In Windows Vista/Longhorn, events related to the security log are also included in the security log.
Audit Log cleared	This report shows events 517 (1102 - Vista/Longhorn). This event identifies when an audit log was cleared. Administrators should not clear security event logs without authorization. Check user performing the attempt field then compare with authorized personnel.
Event Log service errors	This report shows events with type error in the system log with source EventLog. The event identifies errors in the auditing process. Investigate the problems as soon as possible.
Service status report	This report shows the services that run, have failed to start or stopped unexpectedly.
Uptime server report	This report is based on event 6013 (Windows OS Version higher than 6.0). It displays the uptime for each server scanned.

9.9 Events Trend

Report name	Description
Generic event trend per hours	This report shows statistical information from the collected events. It shows the top 10 computers having the highest amount of events and the top 10 users generating the most events. All information is grouped by hours.
Generic event trend per days	This report shows statistical information from the collected events. It shows the top 10 computers having the highest amount of events and the top 10 users generating the most events. All information is grouped by days.
Generic event trend per weeks	This report shows statistical information from the collected events. It shows the top 10 computers having the highest amount of events and the top 10 users generating the most events. All information is grouped by weeks.
Generic event trend per months	This report shows statistical information from the collected events. It shows the top 10 computers having the highest amount of events and the top 10 users generating the most events. All information is grouped by months.

9.10 All critical messages

Report name	Description
All critical Windows Log events	This report shows the most important Windows event logs that need immediate attention. It also shows the top 10 rules that were triggered most frequently by these events.
All critical Syslog events	This report shows the most important Syslog event logs that need immediate attention. It also shows the top 10 rules that were triggered most frequently by these events.
All critical W3CELF events on each machine	This report shows the most important W3CELF event logs that need immediate attention. It also shows the top 10 rules that were triggered most frequently by these events.
All critical Custom Log events	This report shows the most important Custom Windows event logs that need immediate attention. It also shows the top 10 rules that were triggered most frequently by these events.
All critical SNMP Traps	This report shows the most important SNMP event logs that need immediate attention. It also shows the top 10 rules that were triggered most frequently by these events.
All critical Microsoft Sql Server Audit	This report shows the most important Microsoft SQL Server audits that need immediate attention. It also shows the top 10 rules that were triggered most frequently by these events.

9.11 Miscellaneous, Customizable reports

Report name	Description
Generic Windows Event Log report	The Generic Windows Event Log report is a report template that allows wide customization. You can use this template to generate custom reports based on any windows event log, using filtering conditions and grouping modes that are not covered by the default reports.
Generic Windows Custom Log	The Generic Windows Custom Log displays all custom events generated by Microsoft Windows event sources.
Generic SysLog report	The Generic SYSLOG report is a report template that allows wide customization. You can use this template to generate custom reports based on SYSLOG messages.
HTTP activity report	The HTTP activity report is a report template that allows wide customization. You can use this template to generate custom reports based on WELF logs.
Generic W3CELF ISA Log report	The Generic WELF ISA Log report is a report template that allows wide customization. You can use this template to generate custom reports based on WELF ISA logs.
Generic Oracle Audit	The Generic Oracle Audit report displays Oracle server audit events generated by Oracle database event sources.

9.12 PCI DSS Compliance Reports

Report name	Description
PCI DSS Requirement 7.1 - User Account Management	The report will help you achieve the following goals: Find irregular or unusual network account activities, identify administrators who abuse privileges to create or modify accounts and detect patterns of account activities that breach organizational security policies.

Report name	Description
PCI DSS Requirement 7.1 - Security Group Management	Assigning users to security groups, particularly users who have high privileges such as Domain, Schema, or Enterprise Admins, should occur within policy guidelines only, and should make use of established and approved accounts or processes. The report will help you identify the critical operations.
PCI DSS Requirement 7.1 - User Right Assignment Policy Changes	The report shows the changes to user rights assignment policies, with information on who assigned the right, the rights being assigned and the user being assigned the rights. The report helps you determine who has been given access to computers or resources throughout the entire domain.
PCI DSS Requirement 7.1 - System Access Granted/Removed	The report will list for each computer the users that have been granted system access. This will help determine who has been given access to particular computers in the network.
PCI DSS Requirement 7.1 - Failed Attempts to Access Files and Registry Report	The report will list all failed attempts to access files and registry based on the object access events. The report will help you identify unauthorized users attempting to access files that may contain cardholder information.
PCI DSS Requirement 7.1 - Successful Attempts to Access Files and Registry	The report will list all the successful attempts to access files and registry based on the object access events. The report will help you determine if there are unauthorized users who managed to access files that may contain cardholder information. Simply compare the users listed in this report with the list of authorized users.
PCI DSS Requirement 8.5.1 - User Account Management	The report will help you achieve the following goals: Find irregular or unusual network account activities, identify administrators who abuse privileges to create or modify accounts and detect patterns of account activities that breach organizational security policies. The report can also serve as restore data for the unauthorized operations related to user account management - the operations can be undone using the information in this report.
PCI DSS Requirement 8.5.1 - Security Group Management	Assigning users to security groups, particularly users who have high privileges such as Domain, Schema, or Enterprise Admins, should occur within policy guidelines only, and should make use of established and approved accounts or processes. The report will help you identify the critical operations as well as undo operations that were unauthorized or inappropriate.
PCI DSS Requirement 8.5.1 - User Right Assignment Policy Changes	The report will list any change in the user rights assignment policy, with information on who assigned the right, the rights being assigned and the user being assigned the rights. The report helps you determine who has been given access to computers or resources throughout the entire domain. Additionally, the data in this report can help you undo the operations that were unauthorized.
PCI DSS Requirement 8.5.1 - System access Granted/Removed	The report will list for each computer, the users that have been granted system access. This will help determine who has been given access to particular computers in the network. The data in the report can be used to undo the operations that were unauthorized.

Report name	Description
PCI DSS Requirement 8.5.1 - Password Changes Report	Password resets should occur within an approved framework only. Properly configured security audit levels should record password resets in the security event logs and identify those resets that do not follow the correct procedures. The report may contain the following sections: "Change password attempts", "User account password set or reset" and "Changes to directory service restore mode passwords".
PCI DSS Requirement 10.2.1 - All Individual Access to Cardholder Data Stored in Files	The report shows file related activity based on object access events that trigger the corresponding rule in the "Events Processing Rules" section, the "PCI Requirements for Windows OS" group. The report helps you identify the files being accessed and the user accessing the files. In order to have an accurate report, the corresponding processing rules need to be configured to trigger for specific locations (folders) that contain cardholder data.
PCI DSS Requirement 10.2.2 - All Actions Taken by Any Individual with Root or Administrative Privileges	The report shows the activity performed by users having administrative privilege. The product uses advanced techniques to determine for each event log entry: information on the user account that caused the event log entry, does the account have administrative privileges and if not, did the account have administrative privileges at the time the log entry was created.
PCI DSS Requirement 10.2.3 - Access to All Audit Trails	The report shows audit log related activity such as: audit log cleared, successful or failed attempts to access the audit logs and physical (using file managers) access to .evt files.
PCI DSS Requirement 10.2.4 - Invalid Logical Access Attempts	The report shows invalid logical access attempts such as: failed logons, account lockouts, attempts to use unauthorized resources and attempts to use unauthorized applications.
PCI DSS Requirement 10.2.5 - Use of Identification and Authentication Mechanisms	The report lists entries relevant to the use of identification and authentication mechanisms, such as: successful and failed logons, events related to authentication protocols (for NTLM and Kerberos) and events logged by the subsystems handling authentication.
PCI DSS Requirement 10.2.6 - Initialization of the Audit Logs	The report shows information related to the initialization and functionality of the audit logs, such as: failure to audit because of various reasons (event log full, log file corrupt, lack of resources, etc), the errors logged by the event log service and the events signaling that the EventLog service has started or stopped.
PCI DSS Requirement 10.2.7 - Creation and Deletion of System-Level Objects	Level Objects Report for PCI DSS requirement 10.2.7 - The report shows information related to the manipulation of system level objects such as: access to Active Directory objects, deletion of Active Directory objects, deletion of generic objects and the events logged by the Windows File Protection service in case system files are being tampered with.
PCI DSS Requirement 10.4 - Time Synchronization Monitoring	The report shows information related to time synchronization such as: system time changes and activity reported by the Windows Time Service.
PCI DSS Requirement 10.5.1 - EventsManager Activity Audit - Logons	Logons Report for PCI DSS requirement 10.5.1 - The report shows the logons to the main console of EventsManager.

Report name	Description
PCI DSS Requirement 10.5.2 - EventsManager Activity Audit	The report shows the activity that the users have performed on the main console of EventsManager. This activity may include: logons to the console, logoffs, EventsManager configuration changes and access to the log browsers.
PCI DSS Requirement 10.5.5 - Failed Attempts to Access Log Files	The report will list all the failed attempts to access files with the .evt and .evtx extension. It will help you identify unauthorized users attempting to access Windows log files physically, without using the EventLog methods that are being restrictive and logged.
PCI DSS Requirement 10.5.5 - Successful Attempts to Access Log Files	The report will list all the successful attempts to access files with the .evt and .evtx extension. It will help you identify unauthorized users attempting to access Windows log files physically, without using the EventLog methods that are being restrictive and logged.
PCI DSS Requirement 10.6 - Generic Event Trend per Hours	The report shows the trend of the collected events. Including a section showing the top 10 computers with the most events and the top 10 users generating the most events. The events trend chart is divided into hours and the trend of events for each computer is shown individually. The report can be used to determine time intervals where an unusually high number of events were generated.
PCI DSS Requirement 10.6 - Generic Event Trend per Days	The report shows the trend of the collected events. Including a section showing the top 10 computers with the most events and the top 10 users generating the most events. The events trend chart is divided into days and the trend of events for each computer is shown individually. The report can be used to determine time intervals where an unusually high number of events were generated.
PCI DSS Requirement 11.4 - Windows Filtering Platform Events Grouped by Computer	This report shows the network activity generated by each computer running a Window Vista or newer operating system (including the server family), based on the events logged by the Windows Filtering Platform. The report lists for each computer, the connections being made from / to the computer, the port being used, the source /destination address and more importantly, the process that sends /receives information using the connection. This report helps you identify computers that are already compromised or about to be compromised by malware /viruses as well as identify specific network activity.
PCI DSS Requirement 11.4 - Windows Filtering Platform Events Grouped by Destination	This report shows the network activity generated by each computer running a Window Vista or newer operating system (including the server family), based on the events logged by the Windows Filtering Platform. The report shows for each computer, the connections being made from / to the computer, the port being used, the source /destination address and the process that sends /receives information using the connection. This report helps you identify computers that are already compromised or about to be compromised by malware /viruses as well as identify specific network activity.

Report name	Description
PCI DSS Requirement 11.4 - Windows Filtering Platform Events Grouped by Communication port	This report shows the network activity generated by each computer running a Window Vista or newer operating system (including the server family), based on the events logged by the Windows Filtering Platform. The report shows for each computer, the connections being made from / to the computer, the port being used, the source /destination address and the process that sends /receives information using the connection. This report helps you identify computers that are already compromised or about to be compromised by malware /viruses as well as identify specific network activity.
PCI DSS Requirement 11.4 - Windows Filtering Platform Events Grouped by Source	This report shows the network activity generated by each computer running a Window Vista or newer operating system (including the server family), based on the events logged by the Windows Filtering Platform. The report shows for each computer, the connections being made from / to the computer, the port being used, the source /destination address and the process that sends /receives information using the connection. This report helps you identify computers that are already compromised or about to be compromised by malware /viruses as well as identify specific network activity.
PCI DSS Requirement 11.4 - Account Lockouts Report	This report lists all "account locked out" events, including locked accounts due to brute force attack.
PCI DSS Requirement 11.4 - Account Logons Report	This report shows all successful logons grouped by users, enabling you to identify the computers a user has logged on to. The list can be compared with the current authorization list in order to identify authorization breaches.
PCI DSS Requirement 11.4 - Failed Logon Count on Each Computer	This report shows the number of failed logons on each computer, as well as the type of failure, helping you identify suspect access attempts on computers.
PCI DSS Requirement 11.4 - Failed Logons	This report lists the failed logons on each computer in detail, including the type of failure, helping you to identify computers showing suspect access attempts, the users failing to logon and the failure reason.
PCI DSS Requirement 11.4 - Logoffs	This report lists the logoff events on each computer, including the initial logon type. It will help you identify the users successfully ending their sessions.
PCI DSS Requirement 11.4 - Successful Logon Count on Each Computer	This report shows logons by computer and enables you to quickly view the most accessed computers.
PCI DSS Requirement 11.4 - Successful Logons Grouped By Computers	This report lists all successful logons grouped by computers helping you identify the users logging on specific computers.
PCI DSS Requirement 11.4 - Successful logons Grouped by Users	This report lists all successful logons grouped by users, helping you to identify which users are logging on the computers.
PCI DSS Requirement 11.4 - Failed Attempts to Access Files and Registry	The report shows all the failed attempts to access files and registry based on the object access events. The report will help you identify unauthorized users or unauthorized applications attempting to access files and registry that are security sensitive and may indicate a breach or a tampering attempt.

Report name	Description
PCI DSS Requirement 11.4 - Successful Attempts to Access Files and Registry	The report shows all the failed attempts to access files and registry based on the object access events. The report will help you identify users or applications attempting successfully accessing files and registry that are security sensitive.
PCI DSS Requirement 11.4 - Objects Deleted (All)	The report lists all the deleted objects and can help you identify attempts to remove traces of unauthorized activity.
PCI DSS Requirement 11.5 - Failed Attempts to Access Files and Registry	The report shows all the failed attempts to access files and registry based on the object access events. The report will help you identify unauthorized users or unauthorized applications attempting to access files and registry that are important for the main system functionality.
PCI DSS Requirement 11.5 - Successful Attempts to Access Files and Registry	The report will list all the successful attempts to access files and registry based on the object access events. The report will help you identify users or applications attempting to access files and registry that are important for the main system functionality.
PCI DSS Requirement 15.4 - Deleted Files	The report lists the deleted file throughout the network. It will help you identify if there are any critical files being deleted.

9.13 General and Security Requirements

Report name	Description
GCSx Code Of Connection Memo 22 SR8 - Applications Installed / Removed	This report lists the applications that have been installed or uninstalled throughout the network. It can help you identify deployment of unauthorized applications.
GCSx Code Of Connection Memo 22 SR8 - Applications Hanging or Crashing	This report lists the applications that have hung or crashed throughout the network. It can help you identify application misuse or functionality issues.
GCSx Code Of Connection Memo 22 SR7 - User Account Management	The report will help you achieve the following goals: Find irregular or unusual network account activities, identify administrators who abuse privileges to create or modify accounts and detect patterns of account activities that breach organizational security policies.
GCSx Code Of Connection Memo 22 SR7 - Password Changes	Password resets should occur within an approved framework only. Properly configured security audit levels should record password resets in the security event logs and identify those resets that do not follow the correct procedures. The report may contain the following sections: "Change password attempts", "User account password set or reset" and "Changes to directory service restore mode passwords".
GCSx Code Of Connection Memo 22 SR7 - Security Group Management	Placement of users into security groups, particularly users who have high privileges such as Domain, Schema, or Enterprise Admins, should occur within policy guidelines only, and should make use of established and approved accounts or processes. The report will help you identify the critical operations.

Report name	Description
GCSx Code Of Connection Memo 22 SR7 - User Right Assignment Policy Changes	The report will list any change in the user rights assignment policy, with information on who assigned the right, what right was it and to whom was the right assigned. The report helps you determine who has been given access to computers or resources throughout the entire domain
GCSx Code Of Connection Memo 22 SR7 - System access granted/removed	The report will list for each computer, the users that have been granted system access. This will help determine who has been given access to particular computers in the network
GCSx Code Of Connection Memo 22 SR7 - All actions taken by any individual with root or administrative privileges	The report shows the activity performed by users who have administrative privileges. The product uses advanced techniques to determine the following, for each event log entry: what is the user account that caused the event log entry, does the account have administrative privileges and if not, did the account have administrative privileges at the time the log entry was created.
GCSx Code of Connection Memo 22 SR7 - Domain Policy Changes	The report shows the changes to the domain policy of the computers being monitored by EventsManager.
GCSx Code of Connection Memo 22 SR7 - IPSec Policy Changes	The report shows the changes to the IPSec policy of the computers being monitored by EventsManager.
GCSx Code of Connection Memo 22 SR7 - Kerberos Policy Changes	The report shows the changes to the Kerberos policy of the computers being monitored by EventsManager.
GCSx Code Of Connection Memo 22 GR22 - Generic Event Trend per Months	The report shows the trend of the event collection process indicating the trend of event generation across the network. The report can be used to certify that the collected data goes back 6 months or more.
GCSx Code Of Connection Memo 22 SR1 - Time synchronization monitoring	The report shows information related to time synchronization such as: system time changes and activity reported by the Windows Time Service.
GCSx Code Of Connection Memo 22 - Successful Logon Count on Each Computer	This report shows logons by computer and allows you to quickly view the most accessed computers.
GCSx Code Of Connection Memo 22 - Successful Logons Grouped By Computers Report	This report lists all successful logons grouped by computers helping you identify who are the users logging on certain machines.
GCSx Code Of Connection Memo 22 - Successful logons Grouped by Users report	This report lists all successful logons grouped by users, helping you determine what are the computers a certain user has logged on to.
GCSx Code Of Connection Memo 22 - Logoffs	This report lists the logoff events on each computer, including the initial logon type. It will help you identify the users successfully ending their sessions.
GCSx Code Of Connection Memo 22 - Failed Logons	This report lists the number of failed logons on each computer, as well as the type of failure, helping you identify which are the computers showing suspect access attempts.
GCSx Code Of Connection Memo 22 - Failed Logons Count on Each Computer	This report lists the number of failed logons on each computer, as well as the type of failure, helping you identify which are the computers showing suspect access attempts.

Report name	Description
GCSx Code Of Connection Memo 22 - Failed Attempts to Access Files and Registry	The report will list all the failed attempts to access files and registry based on the object access events. The report will help you identify unauthorized users or unauthorized applications attempting to access files and registry that are security sensitive and may indicate a breach or a tampering attempt.
GCSx Code Of Connection Memo 22 - Successful Attempts to Access Files and Registry	The report will list all the successful attempts to access files and registry based on the object access events. The report will help you identify users or applications attempting successfully accessing files and registry that are security sensitive.
GCSx Code Of Connection ISO 27002 10.10 - All Critical Windows events	The report shows all critical Windows events providing information on system errors or security violations.
GCSx Code Of Connection ISO 27002 10.10 - Service status	This report shows the services that run, have failed to start or stopped unexpectedly.
GCSx Code Of Connection ISO 27002 10.10 - Server Uptime	The report shows the uptime of the monitored machines.
GCSx Code Of Connection ISO 27002 10.10.1 - Generic Event Trend	The Generic Event Trend reports show the trend in audit log generation throughout the network. There are reports preconfigured to show the information per days, hours or months.
GCSx Code Of Connection ISO 27002 10.10.2 - Generic Windows Event Log	The report provides very flexible filtering and grouping options allowing monitoring of particular systems running Windows operating systems.
GCSx Code Of Connection ISO 27002 10.10.2 - Generic Syslog	The report provides very flexible filtering and grouping options allowing monitoring of particular systems running Linux /Unix operating systems as well as network devices that are Syslog-enabled.
GCSx Code Of Connection Memo 22 - Deleted Files	The report lists the deleted file throughout the network. It will help you identify if there are any critical files being deleted.

9.14 SOX Compliance reports

Report name	Description
SOX 302.a.4 - User Logon	The report shows logon events generated when a user logs on a computer. The report covers all logon types and includes domain logons irrespective of authentication package being used.
SOX 302.a.4 - User Logoff	This report lists the logoff events on each computer, including the initial logon type. It will help you identify the users successfully ending their sessions.
SOX 302.a.4 - Failure Logons	This report lists the number of failed logons on each computer, as well as the type of failure, helping you identify which are the computers showing suspect access attempts.
SOX 302.a.4 - All Access to Audit Logs	The report shows audit log related activity such as: audit log cleared, successful or failed attempts to access the audit logs and physical (using file managers) access to .evt files.

Report name	Description
SOX 302.a.4 - Object Access - Failed attempts to access files and registry	The report will list all the failed attempts to access files and registry based on the object access events. The report will help you identify unauthorized users or unauthorized applications attempting to access files and registry that are security sensitive and may indicate a breach or a tampering attempt.
SOX 302.a.4 - Object Access - Successful attempts to access files and registry	The report will list all the successful attempts to access files and registry based on the object access events. The report will help you identify users or applications attempting successfully accessing files and registry that are security sensitive.
SOX 302.a.5 - Local audit Policy Changes	The report shows the changes to the local audit policy of the computers being monitored by GFI EventsManager.
SOX 302.a.5 - Domain Policy Changes	The report shows the changes to the domain policy of the computers being monitored by GFI EventsManager.
SOX 302.a.5 - User Rights Assignment Policy Changes	The report will list any change in the user rights assignment policy, with information on who assigned the right, what right was it and to whom was the right assigned. The report helps you determine who has been given access to computers or resources throughout the entire domain
SOX 302.a.5 - Password Policy Changes	Password resets should occur within an approved framework only. Properly configured security audit levels should record password resets in the security event logs and identify those resets that do not follow the correct procedures. The report may contain the following sections: "Change password attempts", "User account password set or reset" and "Changes to directory service restore mode passwords"
SOX 302.a.6 - Account Management	The report will help you achieve the following goals: Find irregular or unusual network account activities, identify administrators who abuse privileges to create or modify accounts and detect patterns of account activities that breach organizational security policies.
SOX 302.a.6 - Group Management	Placement of users into security groups, particularly users who have high privileges such as Domain, Schema, or Enterprise Admins, should occur within policy guidelines only, and should make use of established and approved accounts or processes. The report will help you identify the critical operations.

9.15 HIPAA Compliance reports

Report name	Description
HIPAA 164.308.a.3 - All Access to Audit Logs	The report shows audit log related activity such as: audit log cleared, successful or failed attempts to access the audit logs and physical (using file managers) access to .evt files.
HIPAA 164.308.a.4- Object Access - Failed attempts to access files and registry	The report will list all the failed attempts to access files and registry based on the object access events. The report will help you identify unauthorized users or unauthorized applications attempting to access files and registry that are security sensitive and may indicate a breach or a tampering attempt.

Report name	Description
HIPAA 164.308.a.4- Object Access - Successful attempts to access files and registry	The report will list all the successful attempts to access files and registry based on the object access events. The report will help you identify users or applications attempting successfully accessing files and registry that are security sensitive.
HIPAA 164.308.a.4 - System Startup/Shutdown	The report will list all system startup and shutdown events.
HIPAA 164.308.a.5 - User Logon	The report shows logon events generated when a user logs on a computer. The report covers all logon types and includes domain logons irrespective of authentication package being used.
HIPAA 164.308.a.5 - User Logoff	This report lists the logoff events on each computer, including the initial logon type. It will help you identify the users successfully ending their sessions.
HIPAA 164.308.a.5 - Failure Logons	This report lists the number of failed logons on each computer, as well as the type of failure, helping you identify which are the computers showing suspect access attempts.

9.16 GLBA compliance reports

Report name	Description
GLBA - User Logon	The report shows logon events generated when a user logs on a computer. The report covers all logon types and includes domain logons irrespective of authentication package being used.
GLBA - User Logoff	This report lists the logoff events on each computer, including the initial logon type. It will help you identify the users successfully ending their sessions.
GLBA - Failure Logons	This report lists the number of failed logons on each computer, as well as the type of failure, helping you identify which are the computers showing suspect access attempts.
GLBA - All Access to Audit Logs	The report shows audit log related activity such as: audit log cleared, successful or failed attempts to access the audit logs and physical (using file managers) access to .evt files.

9.17 Microsoft SharePoint reports

Report name	Description
SharePoint - Audit Trail Integrity Events	This report lists all changes done to the audit trail. This includes changes done to logged security events and deletion of log records. (Event IDs: 11, 12, 20)
SharePoint - Access Control Changes	This report lists events related to granting and revoking authority over SharePoint objects. This includes changes done to site collection administrators, group changes and object permissions. (Event IDs: 25 to 30)
SharePoint - Document Update	This report lists events related to document level access. This report enables you to filter the report by the following event IDs: » 13 - Document checked in » 14 - Document checked out » 43 - Document updated » 19 - Object deleted.

Report name	Description
SharePoint - List Update	This report lists SharePoint audit events related to Lists (event ID 44), List Items (event ID 45) and List Item deleted (event ID 19).
SharePoint Container - Object Update	This report lists SharePoint audit events related to site collections (event ID 40), web updates (event ID 41), document libraries (event ID 42) and folder updates (event ID 46).
SharePoint Generic - Object Change Events	This report lists SharePoint audit events related to various object types. These include the following event IDs: » 15 - Child object deleted » 16 - Child object moved » 17 - Object copied » 19 - Object deleted » 21 - Object moved » 22 - Object profile changed, » 23 - SharePoint object structure changed » 39 - Object restored » 45 - List item updated » 51 - Workflow accessed. This report enables you to filter by event ID, specific object, part of title description and URL.
SharePoint - View Events	This report lists events related to document libraries (event ID 48), documents (event ID 47), lists (event ID 49) and other objects (event ID 50).
SharePoint - Audit NOISE	This report lists events that are categorized as noise. In SharePoint, some events are categorized as noise. These give misleading and irrelevant results. LOGbinder SP can be configured to filter these events and group them as event ID 10.
SharePoint - Custom Audit	This report lists custom events created by application developers. LOGbinder SP records these events as event ID 18.
SharePoint - Search	This report provides an audit trail of search queries (event ID 24) executed by users.
SharePoint - Import/Export	This report lists export and import events (56-59) of SharePoint objects.
Information Management Policy Changes	This report lists changes (event IDs 52-55) to Information Management Policy.

10 Troubleshooting

10.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual – most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

10.2 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

10.3 Web Forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

10.4 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

10.5 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: http://www.gfi.com/pages/productmailing.htm.

Index

A

Account Usage Reports 11

C

Configuration settings 4, 22, 23, 28, 31, 38, 41

Custom reports 4, 17, 23, 24, 27, 54

D

Data filters 6, 20

Database source 39, 40, 41

Default reports 3, 4, 5, 7, 11, 12, 13, 15, 21, 49

Distribution of reports 4

E

Email 4, 5, 9, 14, 27, 28, 29, 30, 31, 33, 35, 37, 38

Email settings 9, 29, 37

Export 43, 44

Export reports 5

Exporting 43

F

Failed logons 12, 13, 23, 35, 38

Favorite reports 4, 15, 24, 25

Filter conditions 18, 19, 20, 22

Framework 1, 2, 3, 4, 7, 8

I

Installation 5, 7, 9, 29, 47

L

License 8, 47

N

Navigation button 4, 12, 15, 17, 23, 24, 25, 32, 34, 39, 47, 48

P

Product ReportPack 9, 48

Product Selection drop down list 4, 9, 47, 48

R

Report scheduling 3, 4, 7, 28

S

Schedule activity monitor 33

Scheduled reports 4, 5, 27, 29, 32, 33, 34, 41

T

Troubleshooting 65

X

XML 43, 45